GOOD INFO cyber

COMMUNICATION DE CRISE CYBER

1er Magazine dédié à la communication de crise cyber

L'IA : nouvel acteur de la communication

Trimestriel - Numéro 1 - **25** Euros

SOMMAIRE

Dossier : IA, le quatrième acteur de la communication de crise cyber · Pourquoi le B2A2C change la donne ? · IA émetteur-récepteur et distorsions à grande vitesse · Menaces émergentes · Opportunités : prompts de vérification à tester

Décryptages

La réputation à l'épreuve des crises cyber

L'attaque contre Jaguar Land Rover secoue l'écosystème

Quand Deloitte dérape

Le piège de la communication artificielle

Comment être véritablement vrai ?

Analyse de la communication de Dior

Réglementation

CSRD & communication de crise

Les territoires de crise

Les territoires en crise : le choc

Outils & Checklists

Quels sont les outils de simulation à tester ?

Interview : Myriam Quéméner, Magistrate et experte cybersécurité auprès de Conseil de l'Europe

A retenir

🧠 Nature de la transformation : transition systémique

🌐 Territoire d'impact : socioculturel / médiatique

👥 Parties prenantes : dirigeants / communicants / RSSI

⚠️ Conséquences : obsolescence des plans classiques / distorsion algorithmique

📜 Cadre normatif : IA Act / NIS2

☑ Réflexe stratégique : anticipation & communication IA-compatible

Éditeur : Good Info Cyber — Patrice Remeur. Directeur de la publication : Patrice Remeur — Rédaction : Good Info – Contact : goodinfo @ goodinfo.eu – Publication trimestrielle ISSN : [demande en cours] – Dépôt légal : à parution

© Good Info – Tous droits réservés – Abonnement : collectif (10 personnes) 1 200 euros – Individuel : 160 euros. Tous droits réservés. Reproduction interdite sans autorisation écrite. Ce magazine est conçu selon une approche hybride "humain et IA". Les analyses, la ligne éditoriale et les prises de position sont humaines. l'IA contribue à la recherche documentaire, à la génération d'hypothèses et à l'aide à la structuration.

DOSSIER

Pourquoi vos plans de communication de crise seront-ils obsolètes dès 2026 ?

« L'IA est dans notre quotidien. Mais comment change-t-elle la communication de crise cyber ? Les communiqués sont-ils encore lus par les journalistes ou les clients… ou par leurs assistants numériques devenus des acteurs invisibles et puissants ? Quelles stratégies adopter pour que vos messages restent clairs, fiables et efficaces dans ce nouvel écosystème hybride homme–machine.

- 🧠 Nature de la transformation : obsolescence du modèle séquentiel
- 🌐 Territoire d'impact : temporalité / cognition / écosystème informationnel
- 👥 Parties prenantes : COMEX / communicants / RSSI / IA intermédiaires
- ⚠️ Conséquences : perte de maîtrise du récit / distorsion algorithmique / amplification de la crise
- 📜 Cadre normatif : AI Act · NIS2 · DSA (plateformes et désinformation)
- ☑️ Réflexe stratégique : scénarisation prédictive & messages IA-compatibles dès la conception

Chaque jour, l'IA génère des textes, des images, des vidéos capables d'informer… Elle provoque des bienfaits. Mais elle est aussi capable de tromper ou d'induire en erreur. Elle analyse nos comportements, nos émotions, et répond plus vite que n'importe quel communicant humain.
Dans un tel contexte, sommes-nous prêts à gérer une crise où circulent des deepfakes de dirigeants avant même la première prise de parole officielle ? Avons-nous les moyens de contrer une désinformation automatisée qui envahit les réseaux sociaux en quelques minutes à l'image du mouchoir du Président Macron lors de sa visite en Ukraine ? Et comment intégrer demain ces nouveaux agents conversationnels qui s'adresseront directement aux usagers, clients, partenaires ou médias, parfois avec plus de crédibilité que nos propres porte-paroles ?
La question n'est donc plus de savoir si une organisation sera confrontée à une crise amplifiée par l'IA, mais quand et comment elle y réagira. Les plans de communication de crise cyber, conçus dans un paradigme essentiellement humain et linéaire risquent d'être obsolètes dès 2026.

De nouveaux risques liés à l'IA

Les menaces dites polymorphes – capables d'évoluer en fonction de leur environnement – se développent rapidement. L'ENISA (2023) relève déjà l'apparition de malwares auto-évolutifs et de techniques de désinformation alimentées par IA générative.
Ces menaces échappent aux systèmes classiques de détection, qui reposent sur l'identification de signatures connues.
De plus, les attaques visent désormais les données d'entraînement des IA (empoisonnement de données), rendant les réponses des modèles imprévisibles et manipulées (Europol 2020).
Dans ce nouveau paysage, la communication de crise ne peut plus être pensée uniquement comme une interaction humaine : elle doit inclure la réalité. Les acteurs adverses sont également des IA.

L'obsolescence des stratégies et plans classiques

La plupart des plans de communication de crise actuels reposent sur un cycle séquentiel : analyser la situation, valider un message, diffuser aux parties prenantes par le canal approprié.
Or, l'IA bouleverse ce schéma :
- Les réseaux automatisés propagent rumeurs et désinformation avant même la réaction humaine.
- Les deepfakes brouillent l'authenticité des images et des témoins.
- Les IA conversationnels amplifient de faux récits en quelques secondes, de manière volontaire ou non. Un plan figé, conçu pour des délais humains, est donc dépassé face à la vitesse et à la plasticité des crises amplifiées par les IA.

Apprendre "en marchant"

Les communicants ne disposent pas de recettes définitives. Il convient d'adopter une approche d'expérimentation continue.
Simuler : intégrer dans les exercices de crise des attaques informationnelles générées par IA (fausses notifications, faux communiqués, deepfakes...).
- Tester : mettre à l'épreuve des canaux alternatifs (SMS, intranet dégradé, outils collaboratifs,

conférence téléphonique sécurisée) si les outils numériques sont compromis.

Capitaliser : documenter les réactions, corriger les erreurs, et réintégrer ces leçons dans les dispositifs. Comme l'écrit Erik Hollnagel, la résilience ne consiste pas à suivre un plan unique, mais à "*s'adapter et apprendre en situation*". Et elles sont de plus en plus nombreuses et rapides.

Anticiper avec des scénarios prédictifs

L'autre pilier est l'anticipation par scénarios prospectifs. Cela peut être.

Une attaque par ransomware accompagnée d'une campagne de désinformation automatisée.

Demain, une conférence de presse perturbée par de faux journalistes générés par IA.

Un dirigeant confronté à un deepfake de lui-même diffusé à grande échelle comme c'est le cas pour certains acteurs de cinéma ou personnalités politiques.

Ces scénarios ne sont pas hypothétiques : l'OCDE, via son Observatoire de l'IA lancé en 2025, montre bien les menaces.

Les organisations doivent utiliser la scénarisation prédictive pour tester leur robustesse aux crises émergentes.

Vers une communication homme et IA

Les recherches du professeur Aniket Bera (Université Purdue) montrent que l'IA peut déjà analyser le langage corporel et les émotions pour adapter ses réponses en temps réel (IBM Think). Cela signifie que, dans une crise, certaines interactions avec les parties prenantes passeront par des agents d'IA émotionnels, crédibles et réactifs.

La préparation à la communication de crise doit donc évoluer vers une logique hybride, combinant, des communicants humains garants des décisions, de l'éthique, de la transparence et de l'empathie couplée à des IA de confiance capables de détecter, filtrer et contrer en temps réel les flux de désinformation.

Il convient alors de repenser la communication de crise. Non plus uniquement pour gérer des interactions humaines et médias mais pour désormais intégrer les dispositifs de communication avec les nouveaux médias et acteurs que sont les IA.

La communication IA à IA

Il est aujourd'hui nécessaire d'intégrer la communication machine-to-machine (M2M), où des systèmes — API, bots, agrégateurs, assistants intelligents — échangent les informations sans aucune intervention humaine.

Dans un contexte de crise, ces flux automatisés peuvent déformer, simplifier ou amplifier l'information initiale bien avant qu'elle n'at-

A SAVOIR

> **1271** sites "news /information" générés par l'IA avec peu ou pas de supervision humaine

> **+ 35 %** de hausse de génération de fausses informations contre 18 % un an plus tôt

> **488 incidents** publiquement ont été rapportés affectant banques/institutions financières Selon ENISA, dans le rapport *Threat Landscape: Finance Sector.*

> **179** incidents de deepfake ont été recensés dans le monde au 1er trimestre 2025 selon Surfshark.

teigne les parties prenantes destinataires. Elles créent ainsi des écarts entre la réalité des faits et leur perception.
Les organisations doivent donc anticiper ces distorsions en testant les dispositifs et en mettant en place des garde-fous numériques (contrôles, filtres, signatures électroniques...), afin de garantir que l'authentification du message soit préservée tout au long de sa circulation. Les IA vont nous dépasser et interagir (et elles ont déjà commencé) avec leur propre logique.
Etes-vous prêts à ces nouvelles formes de communication en situation de crise ? Cette expérience sera pourtant inévitable.

L' IA nouvel acteur de la communication de crise

L'IA n'est pas seulement un relais passif, c'est un émetteur et récepteur également source de distorsions.

Récepteur : elle absorbe d'immenses volumes de contenus (communiqués, posts, articles, rapports techniques., images, vidéos..).

Émetteur : elle reformule, contextualise et rediffuse ces informations sous des formes variées (chat, résumé vocal, notification, visuel). C'est un nouveau média dynamique et interactif. Contrairement aux médias traditionnels, l'IA adapte le message à chaque utilisateur. Un PDG recevra une synthèse stratégique, un journaliste un résumé simplifié.

Elle peut transformer le fond (données chiffrées, analyse, langage neutre ou orienté). Elle modifie aussi la forme : texte, voix, vidéo, infographie générée automatiquement.

Elle engage une interaction continue : les usagers questionnent l'IA, qui reformule en boucle, parfois en modifiant l'intention initiale du message.

En cas de crise cyber, cela signifie qu'un seul communiqué officiel peut donner lieu à des dizaines de versions interprétées différemment par autant d'assistants IA. !

Ce basculement change la donne : le public ne consomme plus directement les messages bruts des organisations, mais une version reformulée par une IA. La communication de crise doit donc être pensée non seulement pour convaincre les humains, mais aussi pour être comprise et correctement retransmise par les IA.

Quels changements pour les organisations ?

Préparer une communication de crise cyber ne consiste plus seulement à écrire un communiqué clair et conforme pour les médias ou un mail interne aux salariés.

Il convient désormais de :

- Structurer les messages pour qu'ils soient lisibles par les IA (formats clairs, données vérifiables).

- Anticiper que ces messages seront reformulés et réémis de manière interactive.

- Intégrer l'IA dans le plan de communication de crise comme un acteur à part entière.

Un impératif stratégique

L'IA est un nouveau média dynamique qui redistribue les cartes de la réputation. Ignorer cette réalité, c'est prendre le risque que les messages soient déformés ou concurrencés par des narratifs générés par des machines. En l'intégrant dans la stratégie, le risque peut être transformer en opportunité ! Il s'agit de bâtir des messages adaptés aux humains et aux IA pour préserver la confiance malgré la traduction algorithmique et la vitesse de traitement en vue de prendre la maîtrise d'une communication devenue éminemment interactive.

COMMUNICATION DE CRISE :
AVANT L'IA VS AUJOURD'HUI
AVANT L'IA
PRATIQUES DE COMMUNICATION DE CR/VSE
Cycle séquentiel : analyser → valider → diffuser
Messages centralisés, valides lentement
Dépendance aux mêdias traditionnels
Réponse humaine uniquement
AUJOURD'HUI AVEC IIA
NOUVELLES PRATIQUES DE COMMUNICATION DE CRISE
Intégrer l'IA comme acteur emetteur/récepteur
Messages clairs, structurés pour être compris par l'IA
Fact-checking et simulation en temps reel
Scénarios prédictifs + anticipation rumeure/deepfakes

5 prompts pour vérifier la compréhension de l'IA à vos messages

Il est nécessaire de vérifier votre communiqué ou message et les effets possibles de l'IA sur votre communication initiale. Voici des prompts qui permettent d'anticiper la distorsion des messages et de calibrer la communication pour limiter les risques.

Objectif	Prompt à utiliser	Résultat attendu
Vérifier l'impact médiatique	*"Agis comme un journaliste. Résume ce communiqué en trois phrases pour le grand public."*	Identifier ce qui sera repris en Une
Rassurer les clients	*"Agis comme un client inquiet. Que retiens-tu de ce message ?"*	Voir si le message est clair et rassurant
Vérifier la conformité	*"Agis comme un régulateur. Quels passages peuvent poser problème*	Détecter les risques juridiques
Accessibilité	*"Agis comme une IA grand public. Reformule ce communiqué en langage simple."*	Vérifier la clarté et éviter le jargon
Impact financier	*"Agis comme un analyste financier. Quel effet ce message peut-il avoir sur la perception des investisseurs ?"*	Anticiper les réactions des marchés.

Bonnes pratiques

- Rédiger d'abord une version longue et humaine (juridique, technique, institutionnelle).
- Préparer une version courte IA-compatible (mots simples, phrases factuelles, informations vitales en premier).
- Tester systématiquement les messages avec des prompts avant diffusion.
- Ajouter si possible une signature numérique (C2PA, watermarking, certificat numérique...) pour garantir l'authenticité, voir mettre un flux API ou format JSON pour communiquer en temps réel avec les IA.

Modèles de messages IA-compatibles

Un communiqué destiné à circuler dans l'écosystème numérique doit être court, clair et vérifiable. Voici un exemple pratique d'une banque qui a connu un incident monétique au mois d'aout 2025.

Message officiel

Incident monétique national du samedi 30 août 2025
Les sociétaires et clients de 16 fédérations du Crédit Mutuel ainsi que des banques CIC et Monabanq ont rencontré des difficultés pour effectuer des paiements et retraits par carte bancaire samedi 30 août en fin de journée.

L'incident a débuté à 17h20. Plus précisément, les serveurs d'autorisation des trois banques concernées ont été touchés par une panne interne d'une fonction du système informatique.

Leur rôle est de vérifier, en moins d'une seconde, la légitimité des transactions (y compris la lutte contre la fraude) et la disponibilité des fonds nécessaires pour régler un paiement ou réaliser un retrait d'espèces. Ainsi, les serveurs d'autorisation n'étaient plus en mesure, pendant un temps, de répondre aux demandes émises par les TPE des commerçants ou les distributeurs automatiques de billets principalement pendant 2 heures et 10 minutes.

Dans les minutes qui ont suivi le début de l'incident, une cellule de crise informatique a été mise en place.
Dès 18h00, les équipes avaient identifié la cause de l'incident et engagé les travaux de résolution. La mobilisation des ingénieurs et techniciens informatiques a permis de rétablir le service au niveau national à 19h30 avec un retour à un fonctionnement 100 % nominal à 20h15.

Nous présentons nos sincères excuses aux sociétaires et clients concernés par cette panne inédite pour notre groupe, tant par sa durée que son ampleur.
Le groupe présente également ses excuses aux commerçants pour les désagréments occasionnés.
Toutes les mesures nécessaires ont été prises pour éviter qu'un tel incident ne se reproduise.
Les 25 000 conseillères et conseillers de proximité du groupe se tiennent à la disposition des clients concernés pour les assister en cas de besoin.
Nous les remercions pour leur mobilisation.

Message IA-compatible

Le samedi 30 août 2025 en fin de journée, des clients du Crédit Mutuel, du CIC et de Monabanq ont subi une panne nationale affectant les paiements et retraits par carte bancaire.
L'incident a commencé à 17h20 et a touché les serveurs d'autorisation, essentiels pour vérifier la légitimité des transactions et la disponibilité des fonds.
Durant 2 heures et 10 minutes, de nombreux terminaux de paiement et distributeurs automatiques n'ont pas pu traiter les opérations.
Une cellule de crise informatique a été déclenchée immédiatement pour gérer la situation.
Dès 18h00, l'origine du problème avait été identifiée et des mesures de résolution mises en œuvre.
Le service a été partiellement rétabli à 19h30 et totalement opérationnel à 20h15.
La direction a présenté ses excuses aux clients et aux commerçants pour les désagréments causés par cette panne exceptionnelle.
Elle assure avoir pris toutes les mesures nécessaires pour éviter une récidive et mobilise ses 25 000 conseillers pour accompagner les clients.

Critères	Version humaine	Version IA-compatible
Lisibilité	Paragraphes longs, riches en contexte	Sections courtes, puces, chiffres Un parfait pour résumé
Message clé	Dispersé avec risque de titre anxiogène)	quoi/quand/ impact/résolution
Données	Silencieux risque de rumeur	Doit être formulé prudemment si non confirmé
Action utile	Peu d'instructions concrètes	Ajout "que faire / où suivre" recommandé
Crédibilité	Chronologie solide, cellule de crise	Ajout "autorités informées" et lien statut renforce la confiance

L'IA act impose la transparence

Le règlement désormais en vigueur depuis le 1er août 2024 impose la transparence des systèmes d'IA. Il oblige les entreprises à garantir la fiabilité des contenus produits ou relayés par des intelligences artificielles. Ainsi, une communication mal calibrée, ambiguë ou non vérifiée peut être considérée comme non conforme aux principes de l'IA Act, notamment pour manque de transparence. La responsabilité de l'entreprise émettrice pourrait être engagée si elle n'a pas anticipé ce filtre. Les organisations doivent donc intégrer le cadre de l'IA Act dans leurs plans de communication de crise cyber.

Comment faire ?

Il convient de placer dans son communiqué les informations essentielles — faits clés, impact, durée, état actuel et excuses — dans le chapeau ou le premier paragraphe, avant les détails techniques ou contextuels.

En effet, les IA (comme ChatGPT, Perplexity, Copilot ou Google AI Overviews) coupent, résument ou extraient automatiquement les premiers blocs du texte pour en faire des synthèses rapides. Cette structure permet ainsi de réduire les risques de mauvaise interprétation. À cet égard, le communiqué de presse publié par CrowdStrike lors de la panne mondiale de juillet 2024 est un exemple remarquable.

Par ailleurs, il est nécessaire de signaler explicitement le recours à l'IA lorsqu'elle est impliquée. Cela peut passer par la mention de son rôle (ex. détection automatique, scoring, analyse de données...) et l'indication des mesures de supervision humaine prévues.

Enfin, pour assurer l'authenticité et la confiance, le communiqué doit indiquer clairement qu'il est signé numériquement et qu'il est possible d'en vérifier l'origine et l'horodatage avec une signature électronique par exemple. Ainsi, avec l'IA Act, la communication de crise ne relève plus uniquement du service communication ou de la direction générale : elle implique désormais l'ensemble des directions — juridique, DSI, RSSI, et communication — qui doivent travailler de concert pour garantir transparence, conformité et fiabilité.

Google AI Overviews critiqué pour ses déformations

Plusieurs organisations ont déjà pointé du doigt les réponses trompeuses de Google, allant des hallucinations à la diffusion de contenus inexacts. Saisie en août 2025, la Commission européenne a confirmé avoir exigé des explications à Google.

Deux demandes d'information ont été adressées : l'une sur l'accès aux données pour les chercheurs, l'autre sur les mesures prises par Google pour limiter les risques liés à l'IA générative, notamment les hallucinations, la propagation virale de deepfakes et la manipulation automatisée de services pouvant induire les électeurs en erreur.

La Directive sur les services numériques (DSA) est censée contenir la désinformation des IA.

IA : 1 réponse sur 2 est déformée

L'étude publiée le 23 octobre par l'Union européenne de radio-télévision (UER) et menée par la BBC révèle un constat majeur : 45 % des réponses produites par les assistants IA sont déformées ou erronées.
Les journalistes ayant conduit l'évaluation ont interrogé ChatGPT, Copilot, Gemini et Perplexity sur 30 sujets d'actualité, générant près de 3 000 réponses, puis évaluées selon des standards journalistiques classiques (exactitude, sourcing, contextualisation).

Des résultats qui confirment la problématique de communication avec les IA

1 réponse sur 3 a une attribution absente, trompeuse ou incorrecte.
20 % sont des erreurs factuelles majeures : hallucinations, données obsolètes.
Quant à Gemini dans 76 % des cas les résultats sont plus désastreux, soit plus du double des autres outils.
La confiance accordée aux IA par les utilisateurs dépassent la fiabilité et l'exactitude réelle.

Un passage de la technique au risque de perception

Dans un contexte de crise, la réalité ne se joue plus sur les faits, mais sur la perception instantanée des tiers.
Or l'IA est en train de devenir, pour des millions de citoyens, la porte d'entrée par défaut vers l'information — y compris avant tout relais officiel ou sources établies.
Cela signifie qu'en cas d'incident, l'IA peut raconter votre crise avant vous et contre vous.
Trois bascules sont déjà observables :
Auparavant, quelques émetteurs faisaient l'information. Aujourd'hui une disparité d'émetteurs diffusent en temps réel avec des IA qui auto-génèrent des contenus ou les hiérarchisent.
Avant l'information était vérifier avant d'être publiée. Aujourd'hui elle est publiée sans vérification.
Aujourd'hui la déformation précède la vérité alors qu'auparavant l'information apportait la charge de la preuve avancée. Ce n'est plus le cas. L'information et les preuves doivent être fournis pour démentir et réparer. Mais le mal est fait.

Pourquoi cette évolution devrait inquiéter COMEX, communicants et RSSI ?

Outre que l'IA déforme, lorganisation perd la maîtrise du sens et la confiance, systématiquement. La désynchronisation provoqué par le public qui "sait" avant l'interne provoque une crise interne et externe de manière simultanée. Le décalage entre la réalité perçue et la vérité factuelle provoque l'altération de la confiance et de la réputation.
En pratique, une crise IA-augmentée n'est plus une crise classique. Elle provoque une crise collective, individuelle augmentée par l'IA. Elle est plus rapide, moins maîtrisable et repose sur une perception humaine et algorithmique, non humaine.

Les réponses possibles

La maîtrise ne repose plus sur l'action préparatoire de démentis et une communication préventive permettant de tenter de prouver.
La mise en place de Gouvernance du récit avec une autorité documentée, des faits et des informations préétablies ou preuves enregistrées.
Des réponses vérifiables immédiatement et un corpus certifié.
La nouvelle question clé pour les dirigeants est désormais "Que va dire l'IA à ma place si je ne dis rien ?" Pour la première fois de notre histoire, le silence ne protège plus. Il est immédiatement comblé par une IA qui improvise — parfois faux, parfois dangereux — mais toujours perçu comme crédible.

Le CEPD rappelle l'enjeu de la communication de crise

Le Comité Européen de la Protection des Données (CEPD) vient de publier les résultats de son exercice PATRICIA II, dédié à la gestion des violations de données personnelles dans un contexte de cyberattaque.

Son rapport d'exercice met en lumière un enjeu central : la communication interdisciplinaire. Lors d'un incident, les équipes IT, sécurité, juridiques et DPO travaillent souvent en parallèle, avec des terminologies et des logiques différentes. Les résultats sont désastreux et provoquent des pertes d'informations, alimentent des incompréhensions et génèrent des délais critiques.

Les axes de progrès

Le CEPD à travers cet exercice recommande une transformation profonde des pratiques.

Il suggère de :

1. Créer une compréhension commune et des canaux de communication clairs en formalisant qui parle à qui, quand et comment, via des protocoles internes et des circuits d'alerte traçables. L'objectif est d'éviter les silos et la confusion dans les premières heures de crise.

2. Normaliser le vocabulaire et les messages partagés. Il s'agit d'élaborer un glossaire et langage commun avec une même réalité par exemple, pour les termes « incident », « violation », « notification ». L'ambition est de parler d'une seule voix en interne… et face aux autorités (CNIL, EDPS, usagers…).

3. Aligner les outils et formulaires internes. Harmoniser les formulaires et mes processus de signalement entre DPO, IT et RH est absolument nécessaire pour fluidifier la circulation des informations et documenter la décision.

4. Former ensemble, agir ensemble. Il convient d'organiser des exercices conjoints DPO–RSSI–Juristes–Direction, basés sur des scénarios réalistes pour renforcer la coordination humaine et la réactivité en communication de crise.

Le CEPD montre que la communication n'est pas un simple réflexe de crise. C'est une compétence à la fois de la cyber et de conformité, au même titre que la sécurité ou le juridique.

Elle conditionne la qualité juridique et la notification aux régulateurs et parties prenantes. Elle influence la réputation et la perception publique. Elle détermine la vitesse de reprise d'activité. Elle protège la confiance et réputation.

DECRYPTAGES

« Victime d'une violation de données, Dior connait une crise cyber. Dans l'univers du luxe, où la réputation est clé, un tel incident peut-il éroder la confiance des clients et peser durablement sur la valorisation du groupe ? La stratégie de communication choisie permet-elle de protéger le capital immatériel de la marque et la valeur de la maison Dior ?

- Nature de la crise : fuite de données
- Territoire d'impact : marque / réputation / socioculturel
- Parties prenantes : clients haut de gamme / régulateurs / marchés
- ⚠ Conséquences : défiance / judiciarisation / atteinte internationale
- Cadre normatif : RGPD · PIPL (Chine) · US State Laws (data breach)
- ☑ Réflexe stratégique : communication en 3 temps + assistance immédiate

DIOR : Analyse d'une crise

26/01/25 : intrusion dans les systèmes.

7/05/25 : découverte de la violation.

mi-mai 2025 : communication publique

18/07/25 : notifications officielles aux clients aux US

26/08/25 : Class actions

9/09/25 : Sanction Chine

Le 26 janvier 2025, la maison Dior a subi une intrusion dans ses systèmes informatiques. L'incident n'a été découvert que le 7 mai 2025, avant d'être communiqué publiquement à la mi-mai. Il est probable que Dior ait respecté l'exigence de notification à la CNIL après le 7 mai, même si la date exacte de notification n'a pas été rendue publique.

Aux États-Unis, la notification a été réalisée le 18 juillet. Chaque État dispose de ses propres règles : en Californie, les lettres de notification aux clients doivent être précises et inclure des mesures d'assistance, ce qui explique un délai supplémentaire. Le message est authentifié par un QR code.

Les informations publiées par Dior et déposées auprès du procureur général de Californie confirment que des données personnelles de clients ont été compromises, mais que les données de paiement n'ont pas été affectées.

La communication officielle est claire, et la stratégie consistant à fournir immédiatement les éléments essentiels a permis de rassurer rapidement. La maison de couture a précisé d'emblée qu'aucune donnée bancaire n'était concernée. Dior a également présenté ses excuses.

Une assistance immédiate

La marque a offert à ses clients 24 mois gratuits du service Experian IdentityWorks incluant une surveillance de crédit, une assurance contre l'usurpation d'identité et une assistance téléphonique dédiée. Dans l'univers du luxe, où la valeur client est élevée, cette mesure constitue un véritable investissement réputationnel.

Les risques juridiques

Cependant, le délai de notification reste long, et le calendrier a pu laisser place à des rumeurs. Certains États comme le Texas et Washington exigent une divulgation dans un délai de 30 jours. Ce retard pourrait exposer l'entreprise à des sanctions réglementaires.

Aux yeux de l'opinion, ce délai peut être perçu comme un retard injustifié, voire une dissimulation. Aux États-Unis, les avocats peuvent soutenir que les clients auraient dû être informés plus tôt pour protéger leurs données.

DIOR : Analyse d'une crise

L'entreprise peut justifier ce délai par la complexité de l'enquête forensique, la coordination entre plusieurs législations (Europe, États-Unis, Asie) et la préparation de différentes mesures compensatoires.
Toutefois, d'un point de vue réputationnel, ce décalage nourrit l'idée d'une lenteur, voire d'une rétention d'information.

Manquement à la conformité

Par ailleurs, le 26 août, trois plaignants ont déposé plainte, accusant Christian Dior de ne pas avoir correctement sécurisé et protégé leurs données.
À cela s'ajoute un volet particulièrement sensible en Chine, où les autorités reprochent à Dior d'avoir transféré illégalement les données personnelles des utilisateurs vers son siège en France.
L'entreprise n'aurait pas réalisé l'évaluation de sécurité requise pour les transferts transfrontaliers, ni signé de contrat standard d'exportation de données personnelles, ni obtenu de certification de protection des données. Selon le régulateur chinois, les utilisateurs n'auraient pas été pleinement informés de la gestion de leurs données à l'étranger, ni renseigner formellement pour donner un consentement explicite.
Cette situation place Dior dans le viseur de la réglementation chinoise sur la cybersécurité et la protection des données (PIPL). L'incident a révélé une non-conformité.
La maison de couture aurait payé l'amende dont le montant reste inconnu.
La communication aurait pu être structurée en trois temps :

- un premier message dès la découverte pour assurer la conformité réglementaire et informer sans entrer dans les détails, accompagné d'une Foire aux questions (FAQ) ;
- un deuxième message complet après l'enquête ;
- enfin, une communication de suivi pour témoigner de la transparence et de l'engagement dans la durée.

Dior n'a pas trouvé le juste équilibre entre conformité réglementaire et maîtrise du risque réputationnel. Les poursuites judiciaires entretiennent la crise, et plusieurs médias titrent déjà sur ses conséquences.
Aujourd'hui, Dior est confrontée à un risque financier réel de plusieurs millions d'euros, mais surtout à une crise réputationnelle prolongée par la judiciarisation. La stratégie à adopter désormais repose sur une transparence radicale, une communication claire sur le renforcement des mesures de sécurité, et un accompagnement pédagogique pour limiter l'effet boule de neige.
L'affaire illustre la complexité des crises cyber à l'ère de la mondialisation. Une seule intrusion informatique a déclenché une réaction en chaîne, exposant la maison de couture à des obligations différentes selon les juridictions.
Cette multiplication des cadres réglementaires transforme chaque incident en une crise mondiale, où l'erreur d'un côté de la planète alimente des risques financiers, juridiques et réputationnels ailleurs.
Les entreprises victimes se retrouvent ainsi face à un triple défi :

- regagner la confiance de ses clients,
- rassurer les régulateurs
- et convaincre les marchés que leur gouvernance numérique et leur responsabilité numérique sont à la hauteur.

Dans le secteur du luxe, la valeur repose sur l'image et la fidélité. L'onde de choc dépasse largement la seule question de cybersécurité.
Elle interroge directement la capacité d'une marque à conjuguer conformité, communication, transparence et réactivité sur le territoire numérique, par nature transverse.

Diagnostics

Points forts

Communiqué clair : faits essentiels annoncés (intrusion, périmètre, pas de données financières).

Mesures de protection clients : offre de 24 mois gratuits d'Experian IdentityWorks (monitoring crédit, assurance, assistance).

Coordination avec les autorités : CNIL et autorités américaines

Présentation d'excuses publiques et page dédiée sur Dior.com.

Support client et hotline dédiée

Points perfectibles

Délai de notification : intrusion en janvier, découverte en mai, notification clients US en juillet. Le délai est défendable juridiquement, mais perçu comme trop long côté réputation.

Granularité par région : manque d'un tableau clair distinguant données affectées en Europe/US/Asie.

Violation grave en Chine de la PIPL (Personal Information Protection Law) : transfert illégal de données vers la France sans évaluation de sécurité ni consentement explicite.

Sanction administrative qui a été annoncée le 9 septembre 2025.

A éviter

Trois class actions aux US déjà déposées qui entrainent un risque juridique, financier et réputationnel fort.

L'établissement ne communique sur **aucune mesure de renforcement de la sécurité ou de sa conformité** notamment en Chine.

Silence sur les manquements et laisse le récit aux autorités ou autres.

Dior donne l'image d'une **marque vulnérable** et ne propose pas de mesures.

Coûts plusieurs millions d'euros probablement.

Informations fragmentées auprès des médias et judiciarisation de la crise.

Recommandations d'actions possibles

Transparence : publier un rapport détaillé post-incident : mesures prises, plan de renforcement...

Communication en 3 temps :

Phase 1 : notification immédiate et sobre, pour montrer la réactivité.

Phase 2 : communication pédagogique après enquête (FAQ, infographies sur les mesures correctives).

Phase 3 : suivi régulier auprès des clients et investisseurs avec des preuves de l'amélioration continue.

Conformité : mettre en place un programme de conformité PIPL et annoncer publiquement la mise en conformité.

Communication proactive pour transformer la crise en opportunité en affichant Dior comme une marque engagée dans la protection des données notamment avec une campagne de pédagogie auprès des clients.

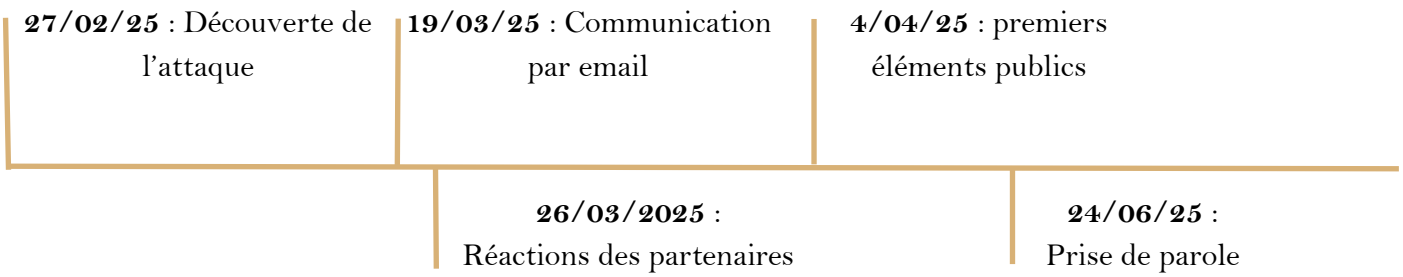
Formation et gouvernance : renforcer la préparation interne (simulation de crise cyber, cellule de communication dédiée, coordination juridique/médias).

DECRYPTAGES

La réputation à l'épreuve des crises cyber

« Comment un éditeur français leader a-t-il été dépassé et déclencher un risque pour son écosystème ? Harvest a été victime d'un rançongiciel. Les révélations publiques déclenchent une réaction rapide et défiance de la part d'organisations professionnelles et grands acteurs de l'assurance. Analyse d'une communication tardive.

Harvest : De la cyberattaque à la crise sectorielle et judiciaire


27/02/25 : Découverte de l'attaque
19/03/25 : Communication par email
4/04/25 : premiers éléments publics
26/03/2025 : Réactions des partenaires
24/06/25 : Prise de parole

Le 27 février 2025, l'éditeur français Harvest, éditeur important des logiciels de gestion de patrimoine et d'assurance, est frappé par une attaque par ransomware, attribuée au groupe Run Some Wares. Services interrompus, données publiées le 16 avril par les cybercriminels… CGP et assureurs tels que AXA France, Maif Solutions financières, Eres et CNP Assurances figurent dans les utilisateurs. Comment un incident technique a-t-il pu se transformer en une crise systémique et judiciaire ?

Le poids du silence

L'incident n'a été communiqué officiellement aux clients que le 19 mars, soit 3 semaines après sa détection. Dans un secteur où la confiance est l'actif principal, que coute une communication trop tardive ? Nous allons le voir. L'absence de communication a nourri des récits délivrés par les parties prenantes. Les Associations de professionnels de la gestion de patrimoine publient une lettre ouverte, dénonçant un manque de transparence. L'ANACOFI première instance française de représentation des conseils en gestion de patrimoine, conseils en finance et développement d'entreprises rappelle, quant à elle, aux conseillers leur responsabilité en tant que responsable de traitement. Harvest est sous-traitant au sens du RGPD. Les membres doivent notifier leurs assureurs et la CNIL dans les 72 heures.

Des réactions en chaîne

Puis ce sont les institutions financières qui se plaignent. Le Crédit Agricole et Suravenir (filiale d'Arkéa) déposent plainte, invoquant le défaut de sécurité et manque de diligence. L'ACPR, le régulateur, demande des informations supplémentaires. En effet, ce n'est plus seulement un incident informatique. La situation génére un risque qui touche assureurs, CGP, banques et des professions connexes comme l'immobilier.

Une communication fragmentée

Harvest avait activé une cellule de crise et envoyé

Harvest : De la cyberattaque à la crise sectorielle et judiciaire

des emails à ses clients le 19 mars 2025. Mais le silence prolongé entre la détection et la première communication officielle a laissé la place à un sentiment de dépassement, voire de négligence. De plus, les messages publiés étaient trop techniques, donc peu accessibles aux non-experts. L'absence de page publique officielle a obligé associations et médias à fabriquer eux-mêmes un récit pour expliquer la crise.
L'entreprise ne raconte pas son histoire, alors d'autres le font à sa place. Le risque ? Il réside que leurs versions puissent ne pas lui être toujours favorables.

Conséquences multiples

Ce manque de transparence et de réactivité a fragilisé la réputation de HARVEST. L'éditeur est désormais perçu comme peu fiable. Les clients doutent de sa capacité à protéger leurs systèmes et leurs données.
Un autre temps de communication se développe alors avec la judiciarisation. Chaque parties prenantes doit agir selon ses expositions réglementaire. Or, les retards de communication alimentent la perception d'une rétention d'information. Ainsi, l'incident informatique prend une dimension judiciaire. Les procédures prolonge l'attaque initiale pour ruiner la confiance. Plusieurs éditeurs ont connu de tels incidents et ont réussi une résilience. Progress MOVEit (2023) a connu une vulnérabilité et à immédiatement assurer des mises à jour et délivrer des informations en temps réel ce qui a permis d'éviter des rumeurs et d'être la source officielle.
En 2024, Ivanti a produit des bulletins techniques proactifs et coordination avec les autorités. Harvest en laissant un vide a permis à d'autres acteurs communiquer à sa place devenant ainsi une arme redoutable pour les plaignants.
Une cyberattaque mal gérée sur le plan du calendrier et de la communication ne reste jamais un incident isolé.
Elle devient crise de confiance puis source de contentieux juridiques… et parfois menace existentielle pour l'entreprise. Alors, face à une prochaine mieux vaut écrire son récit à l'avance. La confiance est le principal actif.
L'affaire Harvest montre également que même une PME/ETI est tenue de communiquer comme un acteur systémique.

EN RESUME

Les décideurs auraient du être garants du calendrier et de la transparence.

Leur arbitrage tardif a alimenté la crise.

Les responsables de la communication qui sont en charge de l'architecture du récit ont subi les communications des parties prenantes.

Les RSSI qui sont les traducteurs entre la technique et le stratégique n'ont pas eu les relais pédagogiques et l'effort technique n'a pas été valorisé.

Diagnostics

Points forts

Activation d'une cellule de crise : mise en place d'une cellule informatique pour contenir l'incident et communication directe par emails aux clients et aux supports techniques.

Identification publique de l'attaque : reconnaissance officielle de l'incident par ransomware (attribué à Run Some Wares), ce qui apporte un minimum de transparence.

Coordination avec le régulateur : l'ACPR a été informée et a demandé des compléments, montrant une interaction réglementaire.

Points perfectibles

Délai de communication : attaque détectée le 27 février 2025, première communication officielle que le 19 mars — plusieurs semaines de silence qui a nourri rumeurs et spéculations.

Communication fragmentée et trop technique : messages adressés aux clients mais pas révélés publiquement.

Manque de cohérence et de centralisation : pas de "trust center" ou de page officielle d'information en continu, obligeant les clients et associations (ANACOFI, CGP) à créer leurs propres récits.

Manque de pédagogie : absence de FAQ claire ou de communication vulgarisée sur l'impact réel pour les clients.

Gestion de calendrier défaillante : les annonces tardives (mars/avril) et la publication des données exfiltrées mi-avril ont accentué l'impression de rétention d'informations.

À éviter

Judiciarisation immédiate : plaintes déposées par Crédit Agricole et Suravenir (Arkéa) pour manque de diligence et défaut de sécurité, créant une crise judiciaire qui prolonge la crise technique.

Silence : Harvest a laissé les associations (ANACOFI, CGP), les médias et les plaignants occuper l'espace narratif, perdant la maîtrise du récit. Les médias CGP ont repris les communications des organisations.

Pas de mesures de réassurance : Harvest n'a proposé aucune mesure visible (monitoring, hotline, accompagnement).

Perception de négligence : l'absence de communication proactive a entretenu un climat de défiance durable dans un secteur où la confiance est l'actif clé. Coût réputationnel et financier élevé : les contentieux prolongés, vont dégrader la crédibilité auprès des acteurs bancaires et institutionnels et faire peser des menaces sur les contrats.

Pas de format pour les IA

L'attaque contre Jaguar Land Rover secoue l'écosystème

« *A ce stade, rien n'indique que des données clients aient été volées, mais nos activités de vente et de production ont été gravement perturbées* » annonce le 2 septembre 2025, Jaguar Land Rover (JLR).
Le fleuron de l'automobile britannique et filiale du groupe indien Tata Motors, vient d'être frappé par une cyberattaque d'ampleur inédite.
En apparence, « *LR a été touchée par un cyberincident* ». En réalité, c'est une attaque qui va révéler la fragilité d'un écosystème industriel entier et la dépendance d'un pays à son champion national.

L'attaque bloque la production
Face à l'intrusion, la direction de JLR a pris une décision de couper ses systèmes critiques pour contenir la menace. Cette bonne mesure défensive a toutefois un prix très lourd. Le coût estimé est d'au moins 50 millions de livres par semaine d'arrêt d'activité. Initialement prévue pour durer quelques semaines, l'arrêt de la production est prolongé jusqu'au 1er octobre au minimum. La remise en route est progressive : certaines fonctions informatiques essentielles (gestion des fournisseurs, facturation, systèmes de pièces) sont déjà repassées en ligne. Mais, les usines britanniques et européennes de l'entreprise sont restées partiellement à l'arrêt. Résultat : des dizaines de milliers de véhicules non produits, des concessionnaires incapables de livrer, et une supply chain mondiale désorganisée. La confiance en la marque est fragilisée.

Une communication progressive
L'entreprise reconnaît que des données ont bien été exfiltrées. Entre-temps, la communication reste centrée sur le système d'information sans expliquer les conséquences pour les parties prenantes et grands publics. JLR laisse sans le savoir planer le doute sur l'impact réel. JLR s'est contenté d'annonces laconiques.
Face à l'évidence technique et aux pressions médiatiques, l'entreprise a dû réviser ces messages, reconnaissant des exfiltrations de données, sans toutefois préciser l'ampleur.
Ce manque de transparence et décalage a endommagé la crédibilité. De la même manière, l'absence de « trust center » ou de page publique centralisée pour informer en temps réel a amplifié le sentiment de flou. Mécaniquement, les rumeurs et conjectures occupent le vide informationnel, reléguant JLR en position de suiveur du récit.

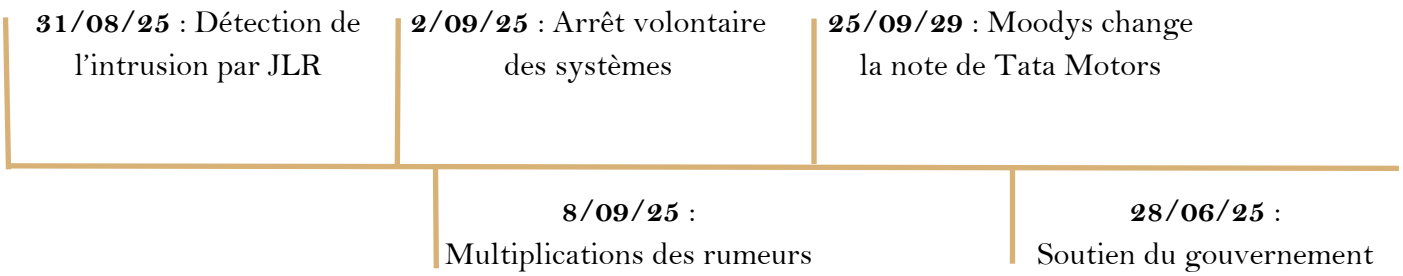
Le gouvernement intervient
Les rumeurs, angoisses et spéculations prennent le dessus. A tel point que la situation pousse le gouvernement de Londres à intervenir. Un prêt garanti de 1,5 milliard £ est délivré en urgence.
Pourquoi un tel soutien ? Parce que Jaguar Land Rover n'est pas une entreprise comme les autres.

EN RESUME

Les décideurs auraient du être garants du calendrier et de la transparence. Leur arbitrage tardif a alimenté la crise.

Les responsables de la communication qui sont en charge de l'architecture du récit ont subi les communications des parties prenantes.

Les RSSI qui sont les traducteurs entre la technique et le stratégique n'ont pas eu les relais pédagogiques et l'effort technique n'a pas été valorisé.


31/08/25 : Détection de l'intrusion par JLR
2/09/25 : Arrêt volontaire des systèmes
25/09/29 : Moodys change la note de Tata Motors
8/09/25 : Multiplications des rumeurs
28/06/25 : Soutien du gouvernement

Elle représente près de 40 % de la production automobile britannique. Elle entraîne dans son sillage plus de 1 000 sous-traitants locaux qu'il convient de préserver.
Elle constitue un pilier stratégique des exportations et de l'emploi manufacturier. L'effondrement de JLR peut provoquer un choc économique et sociale. En réalité, ce soutien financier protège tout un écosystème industriel.
Cependant ce prêt nourrit des polémiques. Il couvrirait un déficit de compétences en ingénierie logicielle, et une déficience de management de crise. Le Financial Times révèle le 12 septembre que JLR aurait aucune assurance cyber.

Des risques multiples pour les parties prenantes

La crise révèle ainsi des vulnérabilités ainsi que celles qui vont bien au-delà de l'entreprise elle-même.
Clients et concessionnaires craignent les retards de livraison, ce qui entrainent frustration et augmente la perception d'une marque peu fiable. Dans l'univers premium, où la confiance et le prestige sont au cœur de la relation, c'est une atteinte directe à l'image.
Les fournisseurs craignent des ruptures de trésorerie, menaces de faillites, dépendance accrue à l'État. Selon le Guardian, certains fournisseurs voient garantir leurs prêts par leurs biens personnels auprès des banques.
Les banques voient les risques de défaillances ainsi augmenter et cherchent des garantis. Certains sous-traitants dénoncent l'absence de communication claire de JLR sur les délais réels.
Sans relation directe avec JLR, ils craignent ne pas être couverts par les flux de soutien public. La catastrophe financière peut arriver.

Dégradation de la note de Tata motors

Les investisseurs manifestent des inquiétudes sur la gouvernance. Moodys abaisse la perspective positive de Tata motors en la passant à négative suite à la cyberattaques.
«*Le changement de perspective de positive à négative reflète notre point de vue selon lequel un rétablissement complet des indicateurs de crédit prendra probablement plusieurs mois*» souligne Sweta Patodia, vice-présidente adjointe et analyste de Moody 's Rating.
«*Le risque cyber liés aux relations avec les tiers est désormais bien pris en compte dans le risque social du cadre ESG* », précise l'analyste. L'arrêt pourrait faire passer les prévisions de 3 milliard de dollars à 850 millions de dollars avec une trésorerie négative.

Une inquiétude de l'Etat et des tiers

La vigilance est renforcée du coté du NCSC britannique (National Cyber Security Centre) et la surveillance accrue sur la conformité aux obligations de notification. Une demande d'informations est lancée.
En interne, les collaborateurs sont angoissés. Les arrêts entrainent stress et inquiétudes provoquant une méfiance vis-à-vis des décideurs. Les effectifs, ont une inquiétude sur la sécurité de l'emploi, réduction temporaire du travail. L'absence de communication et de visibilité sur le redémarrage complet génèrent un climat de tension.
Chaque partie prenante subi la crise et a vécu sa propre crise auprès de ses propres parties prenantes. La situation montre qu'une cyberattaque ne se limite jamais au périmètre informatique.
Jaguar Land Rover pensait affronter une crise technique. Elle s'est révélée être une crise industrielle, financière et réputationnelle. Les cyberattaques par les interconnexions sont désormais des risques systémiques, comparables aux crises financières ou énergétiques.

L'attaque contre Jaguar Land Rover secoue l'écosystème

La communication de crise doit être préparée, transparente et adaptée à chaque public selon différents scénarios. Ce qui a priori manque dans la stratégie du constructeur.
Les erreurs de discours (minimiser, démentir avant de corriger, se réfugier dans le silence) dégradent réputation et confiance. JLR ne se montre pas capable de protéger son écosystème. Par ailleurs le manque d'une couverture d'assurance, signifie que le groupe assumera seul le coût intégral de la crise, affaiblissant sa résilience financière.
La défaillance du manque de communication auprès des acteurs en aval (fournisseurs, sous-traitants) laissera des traces et rendra la relance plus lente et couteuse.

A RETENIR

Pour les dirigeants (COMEX, CODIR)

Risque systémique : une cyberattaque n'est pas qu'un incident technique, elle peut paralyser l'ensemble de l'activité. JLR perd 50 M£ par semaine et est face à un arrêt prolongé de la production.
Responsabilité : le gouvernement britannique a dû intervenir avec un prêt garanti de 1,5 Md£, preuve que la cybersécurité devient un enjeu de résilience voire de souveraineté.
Enjeu réputationnel et financier : Moody's a abaissé la perspective de Tata Motors de positive à négative ce qui génère une perte de confiance des investisseurs.
La cybersécurité doit être gérée au plus haut niveau de gouvernance, avec transparence, anticipation et intégration dans la stratégie globale.

Pour les communicants

Points forts : communiqué rapide le 2 septembre, reconnaissance de l'incident, mention de la coopération avec les autorités.
Points faibles : contradictions sur les données compromises et les exfiltrations confirmées, communication trop technique et lacunaire, pas de canal unique.
Impact : les rumeurs et spéculations ont occupé le vide informationnel, laissant les médias et analystes définir la crise à la place de JLR.
La préparation à une communication claire, pédagogique et multiparties prenantes est nécessaire. Ne jamais minimiser une crise au risque d'être démenti.

Pour les RSSI et responsables techniques

Diagnostic : coupure volontaire des systèmes pour contenir l'attaque et bonne décision défensive logique mais aux effets opérationnels massifs.
Limites : absence de transparence sur la nature exacte de l'intrusion, pas de communication claire vers les partenaires sur la sécurisation future.
Les RSSI doivent intégrer la dimension réputationnelle et financière de leurs décisions. L'absence d'assurance cyber valide a aggravé l'impact.
Il est nécessaire de tester le plan de continuité opérationnelle (PCA) et un dispositif de communication technique simplifiée pour les clients, fournisseurs et régulateurs.

Diagnostics

Points forts

Réactivité initiale : un communiqué a été publié dès le 2 septembre annonçant un cyberincident.

Position officielle assumée : prise de parole publique évitant l'impression de déni.

Lien avec les autorités : Dès le 5 septembre, la coopération avec le National Cyber Security Centre (NCSC) britannique est annoncée

Message de maîtrise : insistance sur la mise à l'arrêt volontaire, donnant l'image d'une décision contrôlée et préventive.

Plan de reprise : communication sur un redémarrage progressif des systèmes, pour montrer un retour vers la normalité.

Points perfectibles

Contradictions dans le discours : annonce initiale affirmant qu'aucune donnée client n'avait été compromise, suivie d'une reconnaissance ultérieure d'exfiltrations. Cela a entamé la crédibilité.

Communication trop technique : centrée sur les systèmes d'information, sans pédagogie ni explication claire des impacts pour les clients, concessionnaires et fournisseurs.

Silence trop long entre deux temps de parole : un mois sans véritable mise à jour auprès des parties prenantes a nourri rumeurs et spéculations.

Pas de canal dédié : Aucune solution est déployer pour centraliser les informations en temps réel.

Manque de gestes visibles auprès des tiers : pas de mesures compensatoires ni d'assistance proposées aux concessionnaires ou acheteurs.

À éviter

Laisser les médias, analystes et hackers occuper l'espace narratif : faute de communication proactive, JLR a subi des récits au lieu de les contrôler.

Absence de transparence sur l'impact financier immédiat : les pertes (50 M£ par semaine) n'ont pas été communiquées par l'entreprise mais révélées par les analystes et la presse.

Fragilisation de la confiance des fournisseurs : absence de communication claire sur la prise en charge de leurs difficultés, alors qu'ils sont essentiels à l'écosystème.

Aucune mise en avant de mesures correctives : sécurité renforcée, renforcement des compétences logicielles, assurance cyber, laissant penser que la vulnérabilité pourrait persister.

Pas de couverture d'assurance : Cette révélation porte atteinte à la crédibilité et solidité de JLR.

Quand Deloitte dérape

Un dossier de 237 pages est remis au mois de juin 2025 au gouvernement australien via le Department of Employment and Workplace Relations (DEWR). Il est publié par le site du gouvernement au mois de juillet.
L'apparence est irréprochable. Le montant de la prestation s'élève à montant de 290 000 dollars environ. Son contenu porte sur un programme lié aux demandeurs d'emploi.
Dès le mois d'aout, un chercheur, Christopher Rudge de l'Université de Sydney a des doutes sur plusieurs informations. Il révèle à la presse que le rapport est « *plein de références fabriquées* » selon AP news, bien que le ton, la structure, et l'apparence de références offrent une apparence sérieuse.

Des sources inventées
et des jugements fictifs
Une première erreur saute aux yeux de l'universitaire. Lisa Burton Crawford, professeur de droit public et constitutionnel à l'Université de Sydney aurai écrit un livre inexistant qui plus est, dont le titre n'était pas le signe de son domaine d'expertise
En approfondissant, des citations attribuées à un juge de la Cour fédérale et des références à des rapports inexistants sont attribués à des experts.
Au moins 20 hallucinations auraient été intégrées par les IA telles quelles, sans aucun contrôle. Humain. Une négligence et situation qui mettent la firme dans une posture difficile.

L'origine : une partie de l'élaboration via IA
Les raisons ? Le rapport a été partiellement généré à l'aide d'une IA. Elle est identifiée comme le modèle GPT-4o via Azure OpenAI.

Des mesures rapides
Deloitte a admis que « *certains notes de bas de page et références étaient incorrectes* » et l'utilisation de l'IA. Le cabinet a présenté des excuses et a convenu de rembourser la dernière tranche du contrat qui serait d'environ 63000 dollars US. Le DEWR affirme que «*la substance de la revue est conservée, et les recommandations n'ont pas été modifiées* ». Dans la pertinence des recommandations, rien de grave si ce n'est la qualité de Deloitte et son métier. Deloitte aurait mise en place des formation complémentaires pour utiliser l'IA de manière responsable. L'entreprise va sanctionner son personnel pour avoir omis de vérifier les informations incorrectes générées par l'IA.

Un tiers de confiance
qui perd confiance
Alors comment une négligence a provoqué une crise de réputation ? Ce qui aurait pu rester un incident s'est rapidement transformé en crise de crédibilité mondiale pour Deloitte. Deloitte est perçu comme un tiers de confiance et pilier de la rigueur, de la vérité comptable, de la transparence. Le tissu d'hallucinations est devenu a fissuré la confiance. Ce n'est pas l'utilisation de l'IA ou les erreurs en soi qui déclenchent la crise mais l'absence de contrôle humain alors que c'est le métier de Deloitte. Ainsi, l'un des champions de

Juin 25 : Remise du rapport au DEWR

Juillet 25 : Publication du document « expert »

Août 25 : Premiers articles critiques

Août 25 : Christopher Rudge découvre des erreurs

Octobre 25 : Version corrigée et remboursement

l'audit et du conseil se retrouve sous le contrôle de l'IA. De par la dimension mondiale de Deloitte, l'affaire a fait les gros titres des grands médias internationaux (Guardian, FT, Business Insider, AP…).
Les confrères ont immédiatement annoncé l'utilisation d'IA et les mesures pour mettre des règles strictes avec un contrôle humain de toutes productions que se soit EY PwC et le BCG.

La sénatrice travailliste Deborah O'Neill, qui participait à une enquête sénatoriale sur l'intégrité des cabinets de conseil, a immédiatement égratigné la réputation : « *Deloitte a un problème d'intelligence humaine. Ce serait risible si ce n'était pas si lamentable. Un remboursement partiel ressemble à des excuses partielles pour un travail de mauvaise qualité* ...Au lieu de faire appel à un grand cabinet de conseil, les acheteurs feraient peut-être mieux de souscrire à un abonnement ChatGPT ». La médiatisation relance au passage le débat sur la rémunération des cabinets...
Quant à l'opinion publique ce qui est intéressant, c'est qu'elle s'est surtout manifestée au sein des réseaux sociaux. Au final, la communication Deloitte maitrisée et narrative aurait suscité peu de couverture journalistique spontanée, signe d'influence avec le paysage médiatique.

Le piège
de la communication artificielle

Cette affaire met en lumière le risque d'un « faux vraisemblable » validée par un tiers de confiance. Le faux devient alors vrai. En effet, cette affaire montre que c'est toute la chaîne de validation, du rédacteur en passant par l'administration, puis aux médias et citoyen.. qui est alors contaminée. Le problème est que le vraisemblable devient alors une « vérité institutionnalisée ou vérifiée». Or c'est totalement faux.

Comment être véritablement vrai ?

L'affaire Deloitte montre la nécessité de vérification dans la communication officielle. La qualité perçue de la communication ou les supports délivrés par des professionnels de l'audit par exemple ne garantit pas la véracité.
Une communication performante si elle ne se fonde désormais pas sur des contenus authentifiés, devient alors potentiellement un vecteur de désinformation involontaire. Voire à terme volontaire.

Des pistes

Pour y remédier trois axes peuvent être déployés :
- Traçabilité : historisation des sources et versions, métadonnées, identification des contenus générés par IA...
- Validation humaine : relecture experte avant diffusion publique et chaine des contrôles et responsabilité.
- Authentification : watermarking, signature numérique, annexes explicatives sur site internet...

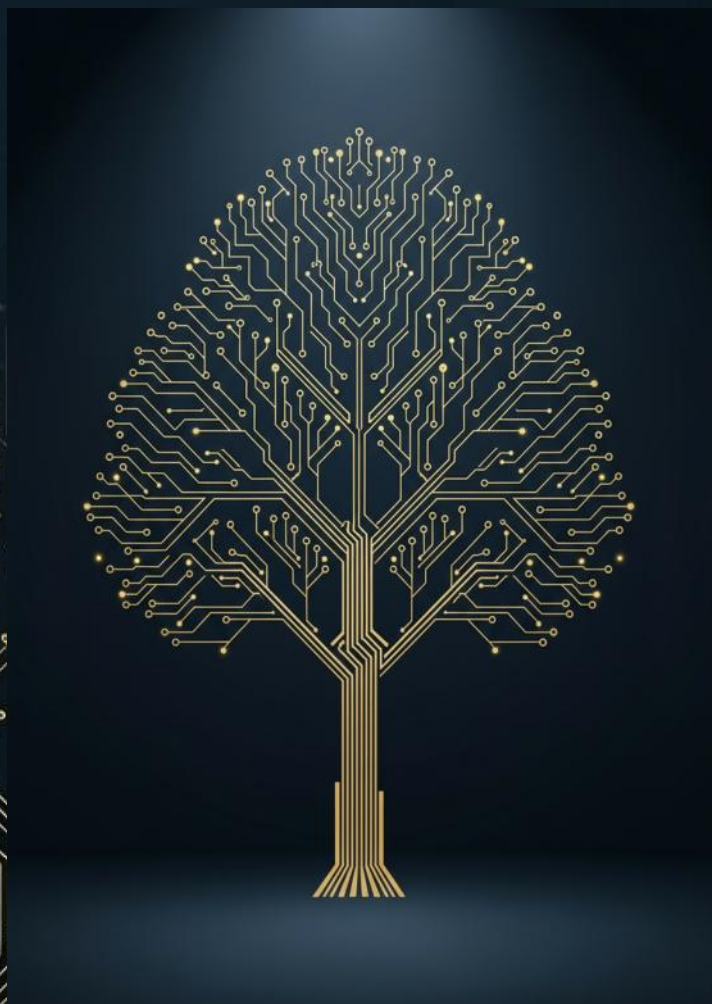
Ces principes doivent être intégrés dans les plans de communication de crise car la perte de confiance n'est plus liée nécessairement à la gravité de l'erreur mais à l'opacité de la réponse ou véracité de la communication. Le vrai défi sera de prouver avec des indices authentifiés.

REGLEMENTATION

CSRD & communication de crise

« A l'heure où la CSRD (Corporate Sustainability Reporting Directive) transforme la publication extra-financière en exigence de transparence stricte, la cybersécurité s'impose comme moteur stratégique de la gouvernance et du développement durable.

Les incidents numériques impactent désormais les bilans financiers, les notations de crédit, la confiance des parties prenantes et le positionnement ESG.



CSRD & communication de crise cyber : quels impératifs ?

Moody's Ratings révèle que "*28 % de la dette collective notée, soit 22 300 milliards de dollars, présente une exposition élevée ou très élevée au risque cybernétique*". Les enjeux sont immenses pour les États et les entreprises. Une mauvaise gestion d'un incident, combinée à une communication mal maîtrisée, peut entraîner une dégradation de la note de crédit. Le cas de Tata Motors après le piratage de sa filiale Jaguar Land Rover en est la triste illustration En quelques heures, ce sont des milliards perdus, une réputation ternie et une confiance fragilisée.

La CSRD change la donne

Face à cette réalité, la Corporate Sustainability Reporting Directive (CSRD), entrée en vigueur en janvier 2024, s'adressant aux entreprises de plus de 250 salariés, sert de catalyseur de transparence et vise à améliorer la durabilité des activités.

La CSRD impose aux grandes entreprises européennes de publier des rapports extra-financiers normalisés, couvrant leurs impacts environnementaux, sociaux et de gouvernance (ESG). Elle introduit une nouvelle exigence de responsabilité : les entreprises doivent désormais rendre compte la gestion de leurs risques dont la cybersécurité. La CSRD demande la gestion des risques cyber dans la gouvernance et au plus haut niveau de l'entreprise mais aussi dans l'ES 1 et 4 par exemple. Ces informations permettent aux parties prenantes de mesurer la trajectoire de l'organisation en la matière.

Ainsi, la CSRD pousse les organisations à améliorer les organisations à mieux préparer leur communication à destination des investisseurs, clients, régulateurs et citoyens. Les organisations doivent fournir sur leur analyse, leur exposition et leurs modalités de résilience pour faire face aux cybermenaces.

Elles doivent intégrer les cyber-incidents et les plans réponse dans la logique ESG, en montrant ainsi leur impact économique, social et environnemental.

Il est nécessaire que les entreprises prépare des dispositifs de gouvernance et de communication de crise capables de limiter la propagation du chaos en cas d'attaque.

En d'autres termes, la CSRD impose aux entreprises de démontrer qu'elles savent prévoir, absorber, gérer et surmonter les crises systémiques.

Dans un contexte où la cybersécurité peut faire basculer en quelques heures la valeur d'un actif, la solidité et la réputation d'une marque, la directive apparaît comme un levier indispensable pour de progrès et de préservation du capital immatériel et extra financier.

Désormais, les organisations ne doivent plus seulement afficher leurs résultats financiers mais aussi rendre compte de leur capacité à anticiper et gérer les risques physiques, naturels ou numériques qui menacent leur pérennité.

Dans ce nouveau cadre, la cybersécurité s'impose comme une dimension centrale. Une cyberattaque n'est pas un problème technique.

Elle peut paralyser l'activité, détruire la valeur financière, provoquer des pollutions environnementales indirectes, et même mettre en danger la vie humaine.

Dans la logique ESG la cybersécurité est appréhendée à travers les filtres environnemental, social et gouvernance. Les parties prenantes vont ainsi regarder l'impact direct sur la société et la santé. Une mauvaise préparation peut entrainer

CSRD & communication de crise cyber : quels impératifs ?

des nuisances aux personnes. Par exemple, l'hôpital de Corbeil-Essonnes a connu une attaque qui a perturbé la prise en charge des patients. La Cour des comptes a reconnu que cela a conduit à des pertes de chance, voire à des décès.
Les attaques peuvent également créer des crises sociales et stress affectant la santé. Les violations de données massives fragilisent la confiance citoyenne et exposent des populations entières à l'usurpation d'identité et à la fraude.

Le pilier Environnement (E)
La cybersécurité peut sembler éloignée des impacts environnementaux. Cependant, une cyberattaque peut entraîner une surchauffe énergétique ou explosion entrainant des dégâts physiques et environnementaux avec des pollutions. Une attaque contre une aciérie en Allemagne a provoqué la destruction d'un haut-fourneau. Une attaque contre Colonial Pipeline en 2021 qui a généré des pollutions graves.

Le pilier S
Les attaques contre des services (eau, énergie, transports) peuvent créer des dommages importants sur les personnes ou environnement. Une cyberattaque laisse des traumatismes aux salariés par exemple et entraine des suspension ou pertes d'emplois. Des violations de données massives fragilisent la confiance et exposent des populations entières à l'usurpation d'identité et à la fraude.
Le pilier Gouvernance (G)
Les agences de notation (Moody's, S&P, Fitch...) évaluent désormais la résilience cyber comme critère de gouvernance.
Les entreprises doivent démontrer la présence de mécanismes de gouvernance : cartographie des risques cyber, cellule de crise, reporting transparent, capacités…

La communication de crise cyber devient un outil de gouvernance indispensable pour prouver que l'entreprise maîtrise ses risques systémiques.

La double matérialité appliquée au cyber
La CSRD repose sur le concept de double matérialité :
- La matérialité financière : pertes économiques, sanctions réglementaires, dégradation de la notation de crédit, hausse des primes d'assurance.
- La matérialité d'impact : conséquences sociales et environnementales pour les parties prenantes et la société telles que la perte de confiance, la fracture ou l'exclusion numérique, les risques numériques, les consommations énergétiques, la fiabilité compromise des données climatiques. Par exemple, une banque victime d'une attaque paralysant ses paiements subit des pertes financières immédiates ainsi qu'à ses clients. Elle provoque également une atteinte sociale en touchant les

A RETENIR

La CSRD impose désormais de documenter la communication et gestion de crise cyber dans les rapports de durabilité, au titre de la gouvernance (ESRS G1).
Les entreprises doivent y décrire leurs procédures d'alerte, de coordination et de transparence lors d'un incident.
Mentionner les exercices de simulation, les rôles des équipes et les enseignements tirés renforce la crédibilité du dispositif.
Une communication claire et rapide réduit le risque réputationnel et améliore la notation extra-financière.

clients privés d'accès à leurs fonds et aux biens convoités.

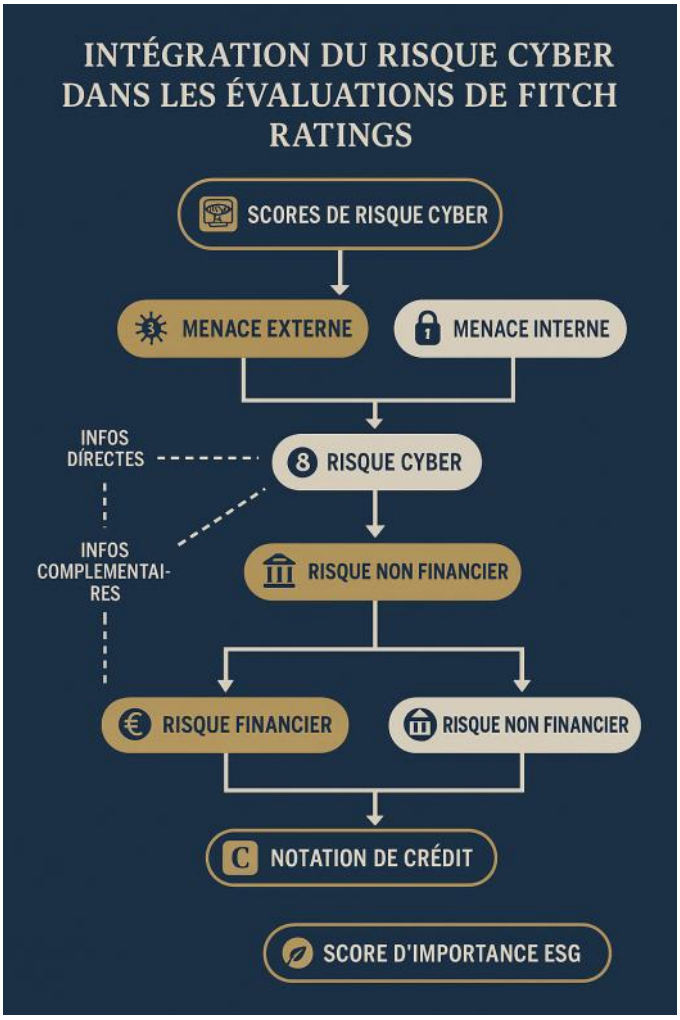
Chaque cyberattaque a donc une triple dimension : financière, réputationnelle et sociétale.

Les impacts réels dépassent largement les bilans financiers. Aux États-Unis, le ransomware contre le pipeline Colonial (2021) a provoqué des ruptures d'approvisionnement en carburant, générant des pénuries, un recours massif à des alternatives polluantes et une hausse temporaire des émissions de CO_2.

En Allemagne (2015), l'attaque d'une aciériste a entraîné la destruction partielle d'un haut-fourneau, illustrant le risque d'accident industriel majeur lié au cyber.

Dans le secteur de l'eau, plusieurs attaques (Floride 2021, Royaume-Uni 2024) ont tenté de contaminer les réseaux en modifiant à distance les niveaux de produits chimiques, mettant en danger la santé publique. Ces exemples démontrent que le cyber n'est pas qu'un risque numérique.

Il a des conséquences physiques, sociales et environnementales, inscrivant pleinement la cybersécurité dans la logique ESG et CSRD.



Notation, réputation et pertes financières : un triangle indissociable

Les agences de notation l'ont bien compris. S&P Global a créé un dataset de 35 facteurs cyber pour évaluer la résilience cyber des entreprises.

Ces indicateurs mêlent données techniques et facteurs réputationnels (impact des violations, volatilité boursière, mesures de diligence, comportements).

Quant à Fitch, l'agence considère que les scores de cybersécurité (issus de fournisseurs ou d'outils) apportent une vue du risque cyber.

Ce risque fait partie des facteurs soumis à l'analyse de crédit. Fitch relie le risque cyber à son cadre ESG qui est alors classé dans la composante "G" (Gouvernance). Il reflète la capacité de l'entreprise à gérer ses données, ses systèmes et sa transparence numérique.

Ainsi, le risque cyber n'est pas un critère isolé dans un silo, mais un facteur parmi d'autres (opérationnel, financier, marché) pouvant influencer la notation. L'évaluation de la résilience cyber et la qualité de la communication de crise sont des indicateurs de stabilité organisationnelle, au même titre que la liquidité ou la dette et la capacité de

CSRD & communication de crise cyber : quels impératifs ?

renflouement et solidité financière. Un discours flou, des informations contradictoires ou un manque de transparence peuvent aggraver la sanction des marchés et des régulateurs.
À l'inverse, une communication claire, proactive et documentée contribue à réduire la perception du risque, et donc à préserver la note de crédit.
Pour un COMEX, cela signifie que chaque cyberincident peut simultanément :
- coûter des milliards (interruption d'activité, amendes, hausse des coûts, démissions...),
- dégrader la notation financière et donc renchérir l'accès aux marchés),
- abîmer la réputation auprès des investisseurs, clients et régulateurs.

Une mauvaise communication de crise ne fait pas qu'aggraver l'image de marque. C'est une mécanique qui fragilise directement la solidité financière et la pérennité de l'entreprise.

Préparer la communication de crise : un levier stratégique

Ainsi, la CSRD n'impose pas seulement de déclarer les risques.
Elle exige de prouver la capacité de réaction. La communication de crise cyber devient donc un instrument de conformité et de performance durable en préservant les actifs et la confiance.

EN RESUME

Les entreprises doivent désormais démontrer qu'elles :
- disposent d'un plan de gestion et de communication de crise cyber,
- qu'elles ont évalué les impacts ESG d'un incident numérique,
- et qu'elles assurent une transparence vis-à-vis des parties prenantes (investisseurs, clients, régulateurs, salariés…).

Vers une communication de crise plus responsable et intégrée

La communication de crise cyber devient ainsi un pilier de la conformité CSRD. Une communication claire, cohérente et factuelle contribue non seulement à préserver la confiance, mais aussi à prouver la bonne gouvernance exigée par les textes réglementaires.

Les organisations les plus matures :
- anticipent les scénarios de crise,
- intègrent les différentes fonctions et responsables dans les cellules de gestion de crise,
- utilisent des outils de simulation et d'entraînement pour tester la coordination entre les acteurs,
- adoptent une stratégie de transparence graduée adaptée aux obligations réglementaires et aux attentes du marché.

A RETENIR

Pour les dirigeants (COMEX, CODIR)

Le cyber est désormais un risque ESG majeur. Il influence directement la notation extra-financière et la confiance des investisseurs. Une attaque devient un événement systémique. Elle affecte la continuité d'activité, la réputation, la relation client et la conformité réglementaire.

La priorité stratégique est la gouvernance et la transparence. Le COMEX doit piloter la cybersécurité comme un enjeu de durabilité, pas seulement technique. L'objectif principal est de passer d'une culture de réaction à une culture d'anticipation. Les scénarios de crise et la communication doivent être testés régulièrement (crash tests, simulations, serious games...).

Pour les communicants

La communication de crise cyber fait partie intégrante du reporting CSRD. La transparence et la rapidité d'information sont désormais des indicateurs de durabilité. Le silence devient un risque réputationnel et ESG ! Un retard de communication ou une déclaration floue alimente les rumeurs et détruit la confiance des tiers investisseurs. Les messages doivent être désormais multi-parties prenantes. Clients, régulateurs, médias, collaborateurs et investisseurs n'ont pas les mêmes attentes. Préparer les outils à l'avance tels communiqués, FAQ, prompts IA validés, messages multi-canaux (site, réseaux, presse…). Chaque minute gagnée vaut des millions en réputation.

Pour les RSSI, DSI

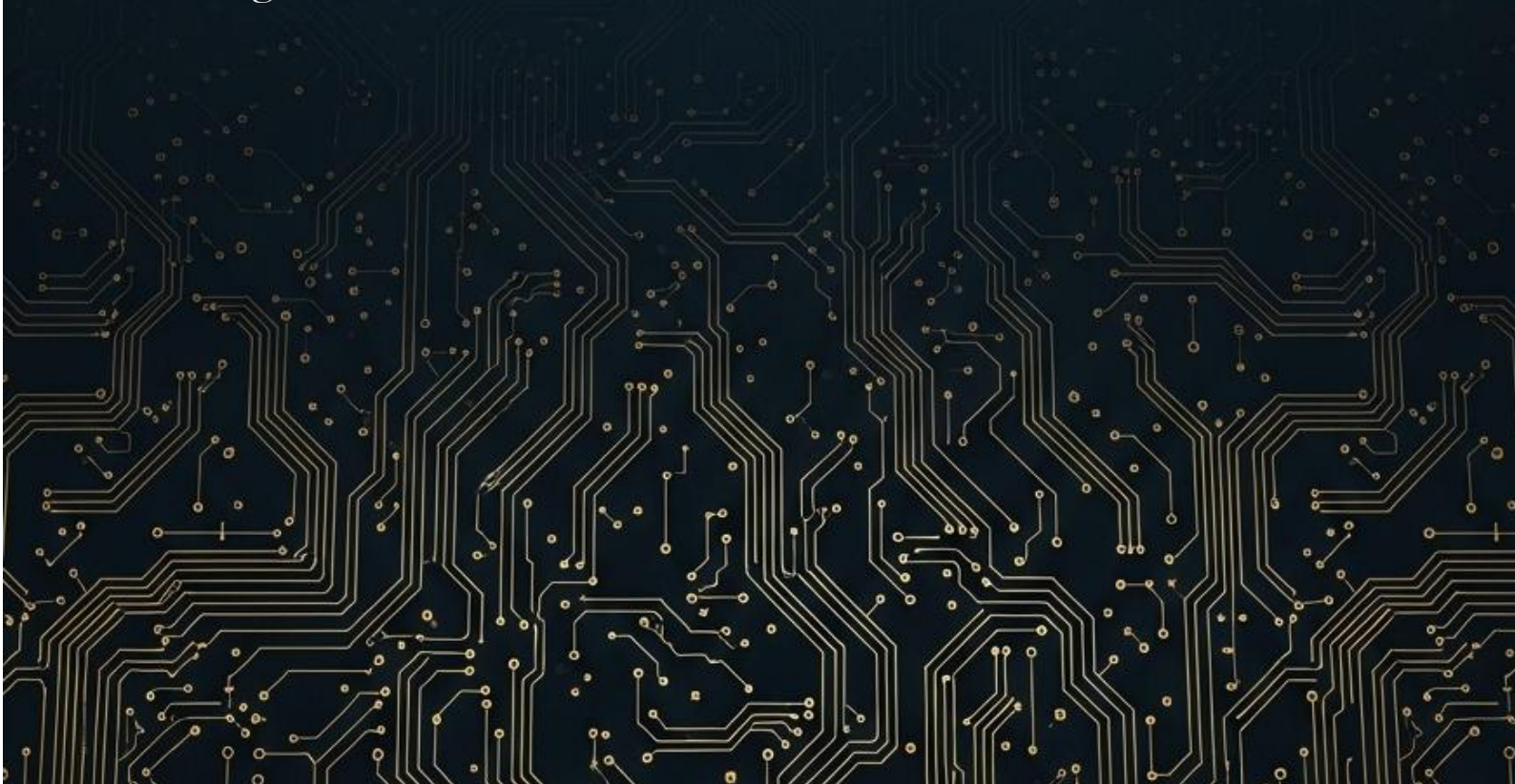
Les obligations DORA et NIS2 imposent une traçabilité totale. Selon les secteurs, d'autres réglementations CRA, CRE… imposent des mesures. Une attaque mal notifiée ou mal documentée devient un risque juridique et de gouvernance. La double matérialité permet de parler le langage du COMEX. Positionner chaque risque cyber sur ses impacts financiers et sociétaux aide à prioriser les investissements et embarquer les parties prenantes. Les exercices conjoints RSSI–Communication sont indispensables. La coordination entre sécurité et communication détermine la résilience collective.

Des indicateurs de suivi peuvent être mis en place pour le rapport CSRD tels que temps moyen de détection et de réaction, les délais de notification clients/régulateurs mais aussi, le taux de participation des dirigeants aux simulations de crise, nombre de participants aux entrainements.

ANALYSE

Pourquoi la communication est-elle multidimentionnelle ?

« Le problème de la communication de crise est qu'elle est multidimensionnelle. Elle touche chaque territoire : médiatique, physique, numérique, de marque, culturel et économique. Elle doit être gérée en simultané et sous haute pression. Sous tous les regards.



Une cyberattaque n'est pas un simple blocage : c'est un choc volontaire malveillant. Elle désorganise, effraie l'ensemble des acteurs et révèle les failles humaines. Pour un faible coût, elle anéantit les systèmes techniques, détruit les processus habituels et génère des tensions culturelles au sein de l'organisation. La communication devient alors l'un des seuls outils de survie collective.

Communiquer sur les différents territoires

Elle touche chaque territoire : médiatique, physique, numérique, de marque, culturel et économique. Elle doit être gérée en simultané et sous haute pression.

Le territoire médiatique :
la guerre du récit

Une crise ne commence plus par un communiqué, mais par un post, une capture d'écran ou un message diffusé par les pirates, à l'image de l'attaque contre Ticketmaster. En mai 2024, cette plateforme, qui compte plusieurs millions de clients dans 32 pays, a provoqué un ouragan d'informations avant même toute déclaration officielle. Les clients, en colère, se sont emparés des réseaux sociaux face à leurs comptes piratés, à leurs billets dérobés, des réceptions d'appels frauduleux… Des témoignages et captures d'écran ont alimenté un récit incontrôlé. La direction a attendu plusieurs heures avant de s'exprimer. Le mal était fait. Le récit n'appartenait plus à l'entreprise. Mais à l'opinion et aux différents publics. Cette mauvaise communication a créé une crise en images, un tremblement émotionnel collectif qui s'est retourné contre la marque.

Territoire physique :
quand la crise secoue le terrain

Une cyberattaque peut avoir un effet concret. La peur devient alors palpable pour les usagers et les équipes.

En mai 2025, le réseau Kettering Health (Ohio, US) a vu ses 14 hôpitaux paralysés par un ransomware et placé par le groupe Interlock. Le manque de transparence a aggravé la situation. Les patients ont été désorientés, les familles se sont inquiétées, les personnels se sont épuisés…

Les perturbations ont été considérables : annulations de procédures, retards dans les soins, systèmes de communication affectés. Certains patients ont été redirigés vers d'autres établissements, entraînant des pertes de chance et des surcoûts en cascades comme des pertes de revenus.

Craignant les arnaques, Kettering a choisi de ne pas contacter directement les patients par téléphone pour éviter les tentatives de fraude, mais cette prudence a également alimenté l'ambiguïté à la faveur des escrocs.

En France, les attaques contre les hôpitaux de Dax ou de Villefranche ont eu le même effet. Problème de communication, patients sans information, agents confrontés à des usagers en colère, déportations des interventions... Ce n'est pas la cyberattaque qui a créé la crise sociale, mais l'absence de communication claire et rapide. Quand l'information n'est pas donnée, la rumeur et l'an-

goisse s'y engouffrent. Une mauvaise communication peut coûter des vies comme l'a montré un rapport de la Cour des comptes.

Territoire numérique :
la crise exponentielle

Les IA, les moteurs de recherche et les réseaux sociaux sont devenus les premiers témoins des crises. Mal gérés, ils deviennent des amplificateurs de désinformation.

Lors de la panne mondiale CrowdStrike, le réseau social X et internautes ont immédiatement relayé l'hypothèse d'une cyberattaque.

Les requêtes Google associées au mot-clé "cyberattack" ont explosé, plaçant l'incident en tête des actualités mondiales. Quelques heures plus tard, CrowdStrike et les autorités ont confirmé qu'il s'agissait d'un simple bug logiciel — mais la perception d'une attaque malveillante, elle, était déjà installée. Quant aux conséquences du disfonctionnements elles ont été importantes partout dans le monde.

Autre cas : la plateforme de trading Zerodha en Inde. Une panne de serveur a été immédiatement interprétée comme une fraude et toutes autres spéculations.

Les forums d'investisseurs se sont enflammés, provoquant un effet domino sur la Bourse. Zerodha a reconnu un bug technique, mais sans en détailler les causes.

Ainsi, l'altération de la réalité a pris le dessus sur la vérité, rendant la restauration de la confiance beaucoup plus difficile.

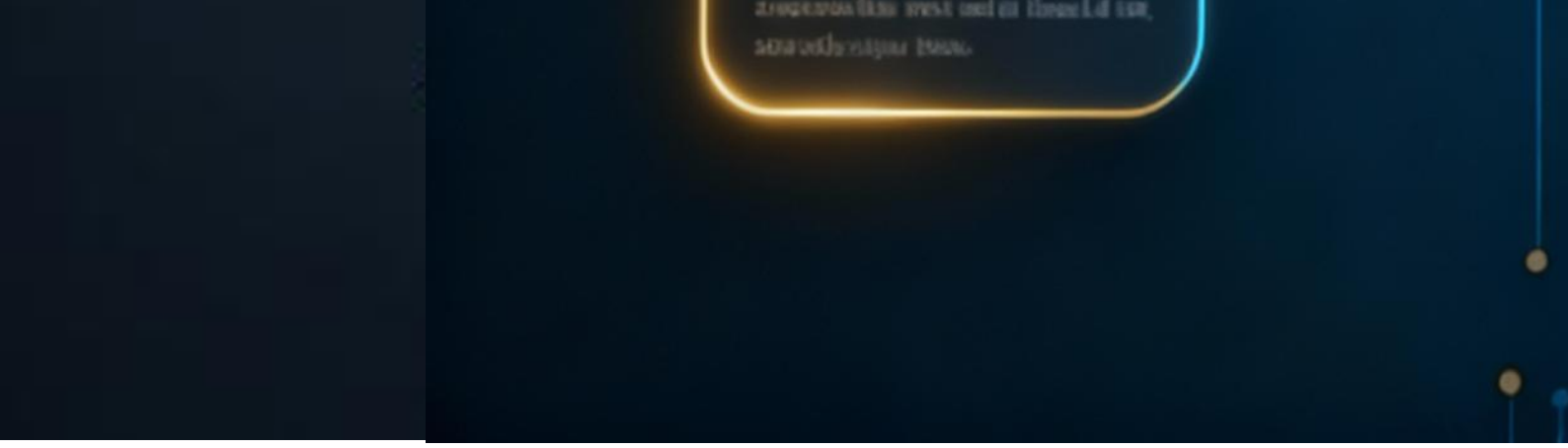
Territoire de marque :
l'épreuve de vérité

Une crise révèle la véritable identité d'une marque. En mai 2025, EasyJet a réagi à une fuite de données contactant directement chaque client avec des excuses avec un ton humain et réactif.

À l'inverse, Cartier, en juin 2025, a reconnu un accès non autorisé à son système. Malgré une communication pertinente, certains clients ont critiqué le manque de détails (durée, cause, nombre de victimes) et le retard du message face aux rumeurs. Dans une crise, le silence initial peut coûter plus cher que l'aveu.

Territoire socioculturel :
valeurs, excuses et réparations

La crise n'a pas la même signification selon les cultures. Elle touche aux valeurs, aux émotions et aux comportements collectifs ou individuels. Le territoire socioculturel est complexe. Il mêle valeurs (transparence, autorité, solidarité…), réflexes culturels (culpabilité, indignation, discrétion...), facteurs sociaux (niveau d'éducation, accès à l'information...) et rapport à la technologie (méfiance, fascination, rejet…). Une cyberattaque agit comme un choc culturel qui va fragmenter le ressenti des acteurs. Ainsi, la crise révèle les représentations profondes qu'une société entretient vis-à-vis de ses institutions ou de ses marques préférées. Les attaques contre les hôpitaux français par exemple ont illustré la fracture entre la culture administrative du secret et la culture ci-



A RETENIR

Pour les dirigeants (COMEX, CODIR)

Les dirigeants sont responsables. Ils doivent anticiper les multiples dimensions.
La communication de crise est une compétence de gouvernance.
Anticiper les 6 territoires de crise : médiatique, physique, numérique, marque, socioculturel, économique.
Décider vite, parler clair. Dans une crise, le silence coûte plus cher que l'aveu.
Soutenir la transparence. Un message incomplet fragilise la confiance de tous.
Coordonner les parties prenantes : communication, sécurité, juridique, RH, régulateurs.
Penser au-delà de l'incident. Une cybercrise peut affecter l'emploi, l'image, la gouvernance et la valorisation.

Pour les communicants

Chaque territoire est spécifique et dispose de canaux, de messages et de cibles différentes. Le rôle du communicant est de prévoir de s'adresser à l'ensemble de ces différents publics et micro opinion. La communication de crise cyber est une discipline d'équilibre : entre empathie, rigueur et réactivité.
Territoire médiatique : être le premier à parler avant que les réseaux ne s'emparent du récit et s'adresser aux leaders d'opinion qui sont désormais dans des médias fragmentés.
Territoire numérique : surveiller les IA, les résumés automatiques et les moteurs de recherche (Google AI Overviews, Perplexity…).
Territoire de marque : humaniser la parole, incarner les excuses, contextualiser les faits et apporter des preuves.
Territoire socioculturel : adapter le ton à la culture, aux émotions, au moment.
Territoire économique : préparer des messages pour les régulateurs, investisseurs, actionnaires et partenaires.
Traduire la complexité. Chaque mot doit rassurer sans tromper, informer sans paniquer.

Pour les DSI & RSSI

La sécurité n'existe pas sans communication.
Partager l'information interne en temps réel. Éviter le cloisonnement technique car c'est l'ennemi de la résilience.
Cartographier les systèmes critiques et les dépendances humaines. Ce sont les premiers leviers de communication utile.
Assurer la transparence technique. Les communicants ne peuvent rassurer sans faits.
Prévoir des canaux de communication de secours. Si les systèmes sont inaccessibles, les informations et données doivent continuer à circuler.
Tester la coordination COMEX–RSSI. Chaque simulation doit inclure un scénario de communication publique.

toyenne de la transparence. Les patients peuvent désormais être enclin à douter de la capacité des services publics à les protéger, voire à les soigner. Les hôpitaux deviennent les symboles d'un système "malade" de virus numériques.

Territoire économique :
la confiance se cote en Bourse

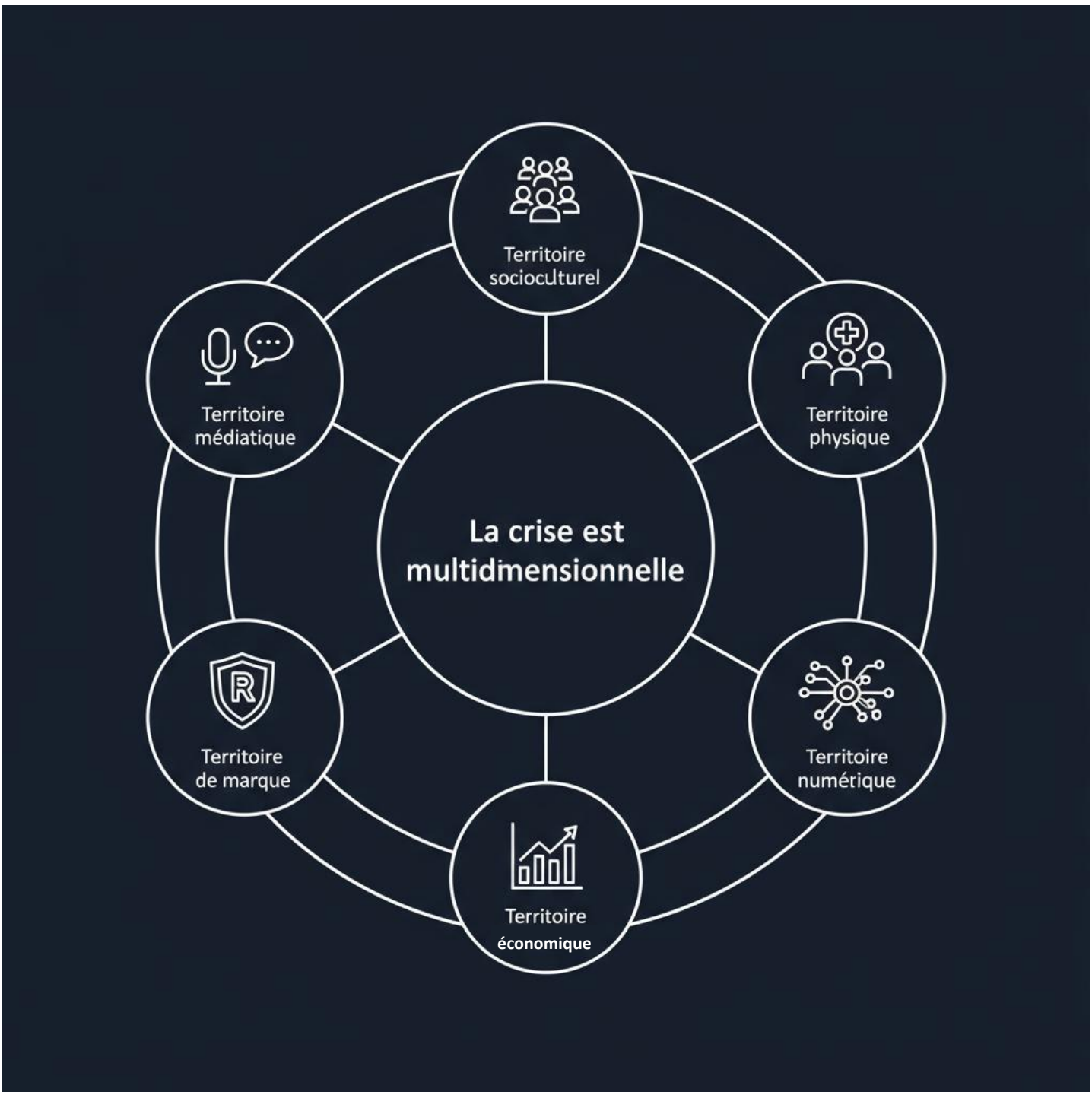
Chaque cyberattaque est aussi un événement économique à part entière. Les marchés sanctionnent plus la confusion que la vulnérabilité. En avril 2025, le groupe américain DaVita, spécialiste de la santé, a perdu près de 10 % en une semaine après un ransomware. Ce n'est pas la brèche elle-même qui a effrayé les investisseurs, mais le manque d'explications claires pendant les premières heures. *"L'ampleur exacte de l'attaque n'était pas connue à l'époque, ni son impact final sur les activités de l'entreprise. Et c'est probablement la principale raison pour laquelle les investisseurs ont abandonné l'action DaVita suite à cette révélation. Les investisseurs n'aiment pas l'incertitude, et l'incertitude reste vive après l'attaque. On ignore encore qui est derrière l'incident, quelles étaient leurs demandes de rançon et,* comme l'entreprise l'a admis, comment DaVita sera affectée. Espérons que nous aurons bientôt des réponses" écrit un analyste du Nasdaq le 18 avril 2025. La confiance perdue entraîne la perte financière.

Anticiper les crises invisibles avant qu'elles ne soient visibles

Ces exemples montrent que la communication de crise est multidimensionnelle et simultanée. C'est un véritable problème que les IA ne savent pas appréhender pour l'instant. Elles peuvent déformer les réalités. La communication ne se résume pas à des communiqués, mais à une orchestration rapide, cohérente et humaine.Chaque silence, chaque mot et chaque minute comptent. Préparer sa communication, c'est anticiper les crises invisibles avant qu'elles ne deviennent visibles.

Les chiffres

Territoire économique : Coût moyen d'une fuite : 4,4 M $ (monde) Huntress/PurpleSec, 2024 - 10,22 M $ (États-Unis) VikingCloud, 2024
Territoire de marque/réputation : 47 % des entreprises frappées rapportent des difficultés accrues pour attirer de nouveaux clients après une cyber-attaque (contre 20 % un an avant) selon Hiscox.
Territoire humain/socioculturel : 88 % des violations seraient causées par une erreur humaine.
Territoire numérique : Les coûts totaux de la cybercriminalité sont estimés à 10,5 billions USD par an d'ici 2025 selon SentinelOne - Le délai moyen de détection et confinement d'une brèche est d'environ 241 jours.
Territoire physique : Jusqu'à plusieurs jours d'annulations médicales, pertes de chance et tensions sociales (Dax, Villefranche, Kettering Health 2025) *Cour des comptes / cas hospitaliers 2024-2025*
Territoire médiatique : Une crise médiatique se déclenche désormais en minutes, pas en heures (CrowdStrike / X, 2024) Analyse sectorielle.


Territoire
socioculturel
Territoire
médiatique
Territoire
physique
La crise est
multidimensionnelle
Territoire
de marque
Territoire
numérique
Territoire
économique

Comment anticiper la crise réputationnelle à l'heure de la responsabilité algorithmique ?

La Cour d'appel de Paris vient de publier une fiche méthodologique inédite sur la réparation des préjudices économiques causés par l'usage d'un système d'intelligence artificielle. Derrière cette apparente technicité juridique, la responsabilité est claire. Lorsqu'une IA cause un dommage, c'est l'organisation qui la conçoit, la déploie ou l'exploite qui est responsable.

Les conséquences pour la communication

Pour les communicants de crise, il ne s'agit plus seulement d'un incident technique, mais d'un risque réputationnel, systémique et social.
Ainsi, la fiche n° 24 de la Cour d'appel de Paris clarifie de quelles manières les juges pourraient analyser les préjudices causés par un système d'intelligence artificielle ? La question n'est plus *"quelle IA a provoqué l'erreur ?"* mais *"quelle gouvernance humaine était en place ?"*. Pour les communicants de crise, l'approche change complètement la manière de préparer, gérer et justifier un incident lié à l'IA.

Le juge ne considère pas l'outil mais regarde l'organisation

Un juge ne va pas auditer l'outil. Il va regarder le cadre et les conditions d'exercices dans lesquels il est utilisé. Il va alors examiner si le risque avait été anticipé avec une réponse suffisante. L'entreprise savait-elle qu'un dommage pouvait survenir ? Qui est responsable et qui assure le contrôle ? Qui surveillait ? A qui revient la défaillance ? Peut-on reconstituer la décision ?

L'entreprise des manquements notamment à son devoir de vigilance ou diligence ?
Cela signifie que le procès lié à un outil IA est déjà un procès de responsabilité et d'organisation avec avant d'être un procès de la technique.

La présomption judiciaire

Derrière ce terme technique, la fiche rappelle un principe fondamental pour apprécier les faits. Le juge peut condamner sans preuve directe, si un faisceau d'indices montre une faute probable ou tout au moins une absence de maîtrise. Ce n'est plus la "preuve absolue" qui compte, mais la cohérence du comportement organisationnel. Ce qui signifie que les décideurs doivent être perçus comme maitre de la situation. La communication fait désormais partie intégrante de la responsabilité organisationnelle.
Plusieurs indices pourraient créer de faisceaux de preuves : absence d'audit préalable, logs inexistants ou incomplets, absence de supervision humaine, gestion tardive ou opaque de l'incident, manque de transparence ou communication imparfaite… Il s'agit d'apporter la preuve de contrôle de l'IA.

Pourquoi est-ce un tournant pour la communication de crise ?

Avant tout incident, il est donc nécessaire préparer des indices et une preuve mise en narration. Il est alors nécessaire de cartographier les IA utili-

sées et la finalité de leurs usages. Par exemple des scénarios sont à prévoir : un système de recommandation "défaillant" dans une plateforme de e-commerce entraînant des pertes de ventes ou une IA intervenant dans un processus industriel et causant un arrêt ou un dommage matériel ou financier…

La gouvernance doit être également inscrite dans les documents publics (RSE, CSRD, rapports, sites...). Un discours de transparence doit être prévu avant d'avoir à s'en défendre. Plus les indices seront révélés tôt plus ils seront solides.

Lors de l'incident prouver la maîtrise et apporter des « preuves », il s'agir de reconnaître le plus tôt possible l'incident pour à la fois limiter les dégâts et sa responsabilité. La reprise et la manière du contrôle humain son nécessaire dans les explications. Enfin, la transparence et la volonté de coopérer et d'assurer une réparation est importante pour démontrer l'état d'esprit à l'ensemble des parties prenantes. Il convient également de raffermir le message de fiabilité en annonçant le renforcement de la surveillance ou de la sécurité mais aussi avec un retour d'expérience public qui montre que l'organisation apprend et se renforce.

Pourquoi le communicant devient acteur de la preuve

Le basculement est fondamental. La communication ne sert plus seulement à défendre l'image, elle devient l'un des éléments probatoires. Une communication tardive est une preuve de défaillance ou de désinformation. Une communication incomplète peut devenir un soupçon ou une faute. L'entreprise qui a un discours d'explication instaure une présomption de maitrise, tout au moins à un moment donné.

La communication permettra de juger la gouvernance. Elle devient alors un acte « juridique » à anticiper.

A savoir :
le cadre réglementaire de l'IA

Le Règlement RIA/AI Act fixe des obligations de documentation, transparence et contrôle selon le niveau de risque, mais ne définit pas de régime de responsabilité civile spécifique pour les dommages causés par l'IA.

La Directive 2024/493 relative à la responsabilité du fait des produits inclut les logiciels dans son champ et considère l'IA comme « produit ».

En pratique, les victimes d'un dommage algorithmique peuvent agir via les régimes classiques de responsabilité civile fondée sur la faute. Peu d'affaires emblématiques sont encore réglées devant les juridictions européennes ou nationales (France, Belgique, Italie…).

Deepfake l'attaque vraisemblable

8h42 – Imaginez que vous êtes à Shenzhen. Vous être dans une salle de réunion confidentielle.
Le service directeur financier vous a demandé de vous isoler pour vous connecter à une visio-conférence "stratégique". Sur l'écran, votre dirigeant apparaît. Même regard. Même posture. Même de voix. Il explique qu'une opération de haut niveau doit être exécutée immédiatement. Il vous demande trois transferts rapides. En moins de 10 minutes vous avez exécuté ces transferts d'un montant total de 26 millions de dollars.
A 9h00 le directeur financier vous appelle au téléphone. La fraude n'a pas seulement contourné la sécurité. Elle a usurpé l'autorité.
Vous comprenez que le deepfake a imité le dirigeant.
Avec les deepfakes l'attaque change. La communication se fait naturellement. Aucune perception d'anomalie apparait. La détection du fake se fait après avoir pris connaissance de l'usurpation.

La charge de la vérité

Les hackers vont faire la publicité de leur action via les réseaux sociaux. Les systèmes de distribution algorithmiques vont privilégier l'engagement et la viralité et ainsi exacerber la propagation de fausses informations tout en entraînant une diminution de la confiance dans le processus de traitement de l'information véritable.
Le faux sera publié avant la vérité. L'IA va véhiculer la perception avant la preuve.

La vraisemblance

Les travaux de recherches de Liu et Yang de l'Université de Shangai par exemple ont montré que les utilisateurs passent par deux étapes cruciales pour évaluer la crédibilité des informations en ligne : l'attention portée aux informations importantes et l'interprétation à des fins de jugement.
Les utilisateurs analysent généralement l'information à l'aide du modèle de vraisemblance. "*En plus de la pertinence, des facteurs tels que la capacité auto-perçue de traitement de l'information, la répétition des messages, l'attention distribuée et les expériences antérieures influencent également la façon dont les individus traitent l'information, affectant ainsi leur auto-efficacité*". Les études de Nightingale ont constaté que seulement 60 % des images deepfake pouvaient être détectées de manière fiable par des observateurs humains. Quant à la capacité de détection des machines les plus performantes elles baisseraient en précision pour chuter à 45% voire aucune détection pour le clonage de voix.
Ainsi, dans un environnement saturé d'images et de signaux faibles. Sans moyen de vérification, l'utilisateur se fit sur ce qui est dit en premier et non plus ce qui vrai. L'image fonde la crédibilité mais aussi l'antériorité. Dans cette mécanique la vérité retardée devient érodée et difficile à rétablir.
La communication officielle à un temps de retard. Elle est réactive à l'information délivrée par les

hackeurs. La communication arrive plusieurs heures après. Les preuves plusieurs jours. Alors qu'il a fallu quelques instants pour que les hackeurs livrent l'information. Les IA ont intégrées l'information en quelques instants. La chaine de réactions à accélérer la diffusion de la fausse information.

Les chercheurs clonés pour leur crédibilité

La bataille se joue alors sur le temps. Le faux reste la seule source disponible dès lors qu'elle n'est pas contredite. Par exemple, dans un article de Nature (2024), plusieurs chercheurs renommés, Kgomotso Mathabe et Viswanathan Mohan, ont été clonés pour promouvoir de faux médicaments. Le deepfake n'a pas attaqué leur réputation. Les hackeurs ont réutilisé la crédibilité des chercheurs pour vendre les faux médicaments. Les véritables chercheurs ont mis du temps à découvrir l'existence même de la vidéo. Les vidéos par leur diffusion à leur insu ont créé du vrai.

Les personnalités sont très ciblées

L'usurpation d'identité des personnalités et dirigeants est une menace à laquelle la plupart des organisations demeurent dangereusement mal préparées. Le Centre d'analyse et de partage d'informations sur les services financiers (FSISAC) avertit que ces attaques marquent "*un changement fondamental : on passe de la perturbation des processus démocratiques à* l'attaque *directe des opérations commerciales".*

Le 13 février 2024, une vidéo manipulée par IA a été détectée. Elle usurpait l'identité vocale et visuelle d'un journaliste de France 24, Julien Fanciulli. Dans cette vidéo, le journaliste affirmait que les services de renseignement ukrainiens auraient eu pour projet d'assassiner Emmanuel Macron et d'en faire porter la responsabilité à la Russie, de sorte à obtenir de nouvelles livraisons d'armes. Ce n'est donc pas la sécurité informatique qui préserve la réputation mais la capacité à donner la vérité et d'expliquer. Sur ce dernier exemple, France 24 a immédiatement publié un article "Truth or Fake" et réalisé une déclaration indiquant que la séquence n'avait jamais été diffusée et a fourni des éléments de vérification (lip-sync, voix, contexte) pour démontrer la manipulation. La chaîne a également replacé la vidéo dans le contexte de désinformation pro-russe, identifiant les canaux de diffusion (VK, Telegram). Le cas a été repris par des fact-checkers indépendants et des bases d'incidents IA (AI Incident Database) qui ont classé l'événement permettant de renforcer la crédibilité de la réponse. La communication doit désormais entre en capacité d'authentifier sa propre voix, son image, ses données ou ses écrits.

Ce qui impose aux organisations de se reconfigurer autour de la preuve pour affirmer la crédibilité. Le Comex devient alors gardien de la crédibilité et le dircom porte les preuves au public.

L'IA et les 3 V de la communication

Comment faire lorsque le temps humain n'est plus aligné par le temps informationnel alimentée par des machines ? Vitesse, vérification, vigilance sont les atouts de l'IA comme accélérateur de la maîtrise en communication de crise. Pendant des années, la communication de crise reposait sur une idée simple : analyser, décider, parler.
Aujourd'hui, une information peut installer une version des faits ou brouiller les cohérences de communication. Dans cet environnement, l'IA n'est pas une option technique, elle devient une infrastructure et un outil nécessaire. L'IA n'a pas vocation à communiquer à la place de l'humain mais de préparer, accélérer et structurer. Elle donne la capacité de répondre vite, juste et de manière prouvable.

Comment l'IA change réellement la communication de crise

L'IA peut détecter avant l'humain. Des signes de détection comportementale peuvent être relevés. Par exemple, des comptes amplifiant une fausse vidéo avant qu'elle ne devienne virale, peuvent être identifiés par des hashtags suspects, des analyses de contenus (polémiques, accusations…), ou volume d'interactions... Les IA peuvent permettre d'avoir l'information avant les médias ou les activistes et ainsi, permettre de répondre au moment opportun ou de manière anticipée.
L'IA offre également un diagnostic immédiat. L'IA par sa capacité à traiter un grand volume de données peut améliorer la compréhension minute par minute. Lors de la fausse explosion du Pentagone, les analystes ont pu répondre en détectant rapidement la source probable en quelques minutes.

Tester les messages auprès d'audiences synthétiques.

L'IA propose des options de messages. L'IA permet de formuler différents messages aux cibles dédiées de manière simultanée sans remplacer l'arbitrage humain. Les suggestions peuvent être immédiates. L'IA réduit ainsi le temps de latence.
L'IA peut tester le message avant publication. La validation des messages peut être réalisée par des tests sur les audiences synthétiques.
Les équipes de communication peuvent évaluer le ton du démenti en s'appuyant sur des modèles simulant l'impact sur :investisseurs, les journalistes financiers, le grand public, les émotions, la crédibilité… L'IA permet alors de passer rapidement de l'intuition à la persuasion.

L'IA authentifie la vérité

L'IA par sa capacité de diffusion peut fournir une preuve visuelle certifiée pour couper la rumeur. Certificats et preuves, sites officiels, publications dans les médias… peuvent être quasi instantanés.
L'IA crée la traçabilité pour protéger le dirigeant
Ce qui change fondamentalement est que chaque décision devient démontrable.
Les organisations peuvent journaliser les sources détectées et messages, les options proposées par IA, le process de décision humaine, les motifs de la décision, préparer la défense juridique, vérifier la conformité...
Les actions de communication assistées par IA deviennent ainsi globales et réactives.

Comment simuler les réceptions des audiences ?

L'IA permet de modéliser virtuellement une population ou un segment d'audience afin de prédire ou d'anticiper ses réactions à des messages, contenus, produits ou scénarios. Par exemple, on crée des « personas » (personnages fictifs) dotés de caractéristiques démographiques, psychographiques, comportements, et de simuler les interactions possibles et leurs réactions face à un contenu donné.
Ce type d'outil permet de concevoir un persona (âge, genre, préférences, contexte), de simuler des réactions, dialogues… via différents modèles.
Ils offrent également la possibilité de vérifier l'influence, la viralité ou l'escalade. Mieux, ils proposent d'évaluer les sentiments ou encore les scénarios les meilleurs. Dans un contexte de communication de crise ces outils peuvent permettre à une organisation d'anticiper la réaction des cibles.

Pourquoi ces simulateurs sont-ils pertinents en communication de crise ?
Ils permettent de réduire les incertitudes. Dans une situation de crise, l'organisation (entreprise, administration, ONG) fait face à des enjeux de réputation, de confiance, de rapidité, de diffusion d'information. Utiliser un simulateur d'audience permet de tester différentes formulations de messages, de multiples canaux, d'élaborer différents scénarios de réponses avant d'entrer dans la réalité.. Cela peut réduire l'incertitude et de conserver les versions les plus pertinentes.

Accélération de la prise de décision
En situation de crise, le temps est un facteur clé. Au lieu d'attendre des panels ou des réactions hostiles ou lentes, un simulateur d'audience peut donner des retours quasi-instantanés (ou au moins beaucoup plus rapides). On peut faire des A/B ou A/B/C-tests virtuels sur les messages à adresser. Les simulateurs d'audience ne se contentent pas de réactions, ils peuvent modéliser les interactions entre agents, les effets d'amplification, les chamboulements de discours, etc...
Même après la crise, l'usage de ces simulateurs permet de tirer les enseignements, de « rejouer » des scénarios, de s'entraîner à la communication sans risque.

Comment utiliser ces outils ?
Bien qu'offrant plusieurs avantages, les simulateurs ne sont pas pour autant des outils magiques. Il est nécessaire de bien définir les personas en cohérence avec les caractéristiques démographiques, culturelles, comportementales de vos publics réels pour avoir une simulation correcte.
Il est également nécessaire d'adapter les scénarios aux spécificités de votre crise : message, canal, timing, niveau d'urgence, type de crise (réputation, sécurité, environnement, juridique…) . Il est également nécessaire de prévoir un protocole de validation. Après diffusion réelle, il est opportun de comparer ce que le simulateur anticipait et ce qui s'est réellement produit, pour calibrer le simulateur pour l'avenir.
Former les équipes communication est également impératif. Même le meilleur outil reste qu'un outil. Il faut que les équipes comprennent les données et informations. Les personnels doivent savoir les interpréter, et intégrer les résultats dans la stratégie.

Les outils offrent la possibilité de combiner simulation et écoute réelle. En effet, la simulation ne remplace pas l'écoute des médias, réseaux sociaux et retours terrain. Elle est complémentaire et permet de gagner en pertinence.
En cas d'utilisation de simulations pour influencer publics, il est nécessaire d'être transparent. Il ne faut pas faire passer une simulation pour un vrai panel. Ces outils entrainent la communication dans une nouvelle dimension pour également gagner en réactivité, en pertinence et en réduction des effets négatifs.

Quels sont les outils de simulation à tester ?

Voici une liste d'outils en partie gratuits pour tester vos communications.

Hélas, nous n'avons pas trouver de solutions européennes pertinentes pour l'instant.

Artificial Societies

Permet de décrire un public cible en langage naturel ou de générer une base de personas à partir d'interactions réseaux sociaux. Elle exécute des simulations A/B de message et retourne des scores, des commentaires et des résumés.

Ask Rally

C'est une plate-forme de simulation d'audience virtuelle, qui permet de tester des contenus, questions et idées avec des agents synthétiques, de segmenter l'audience, de recevoir des votes, feedbacks et analyses.

Socialtrait

Une plateforme SaaS récente (octobre 2025) permettant aux équipes marketing et communication de tester idées, concepts, mais aussi modéliser la communication de crise.

Ces outils ne sont pas exhaustifs et donnent un bon panorama des options disponibles.

Les conseils du trimestre à retenir

Ce que les COMEX doivent préparer dès aujourd'hui

Préparer les preuves
Structurer la parole
Validation de messages courts, vérifiables, IA-compatibles
Entraîner les dirigeants

Exercice trimestriel :
Deepfake PDG
Rupture totale communication interne
Fuite médiatique avant conférence interne

Ce que les DSI doivent préparer dès aujourd'hui

Industrialiser la preuve numérique
Journalisation infalsifiable
Horodatage cryptographique
Export rapide de logs, tickets, chronologie
Procédures d'authentification des messages
La capacité à prouver la résilience informatique.

Architecture de continuité
Canaux internes "mode dégradé" (SMS, audio...)
Kit de communication d'urgence IT
Page statique de crise prête à être activée
Standardiser les messages techniques

Exercices à mener :
Simulation ransomware et extraction de preuves
Coupure totale des outils internes (Microsoft/ Google)
Deepfake d'employé IT ou fausse alerte SOC

Ce que les Directeurs Communication doivent préparer dès aujourd'hui

Préparer la vérité
Référentiel de preuves et sources certifiées
Charte de communication de crise et IA
Kit "narratif" (éléments de langage + preuves + chronologie)
Templates de prise de parole
Double version : humain et IA-lecture
Test systématique des messages par IA (résumé / reformulation / risque)
Veille réputation et détecteurs deepfakes
Scénarisation "silence narratif vs. parole rapide"

Exercices à mener
Conférence de presse simulée avec journalistes et IA
Vidéo deepfake du PDG et rumeur syndicale

INTERVIEW

La transparence sur l'utilisation d'IA est une obligation

« Myriam Quémener Avocat général près la cour d'appel de Paris, magistrat, docteur en droit et experte auprès du Conseil de l'Europe en matière de cybercriminalité analyse les nouveaux leviers réglementaires avec des sanctions renforcées, des obligations de transparence, une responsabilité accrue des organisations et l'émergence de nouveaux concepts face à des réalités fabriquées.

GI : Au niveau français et européen, quelles réglementations ou dispositions sanctionnent aujourd'hui les actes de diffusion de contenus falsifiés, de deepfake ou d'atteinte à l'image ?

MQ : En France , la loi SREN a complété l'article 226-8 du code pénal qui réprimait déjà « le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention ».
Dorénavant, cet article sanctionne également « le fait de porter à la connaissance du public ou d'un tiers, […] un contenu visuel ou sonore généré par un traitement algorithmique et représentant l'image ou les paroles d'une personne, sans son consentement ».
Les termes « traitement algorithmique » désignent ici l'utilisation d'une intelligence artificielle. Ce comportement est réprimé s'il n'est pas fait mention de l'utilisation d'une intelligence artificielle ou si cette utilisation n'est pas évidente.
Des sanctions adaptées sont donc nécessaires afin d'éviter une prolifération de l'utilisation et de la publication des deepfakes. L'infraction mentionnée ci-dessus est punie d'un an d'emprisonnement et de 15.000 euros d'amende. La peine est portée à deux ans d'emprisonnement et à 45.000 euros d'amende lorsque le deepfake a été réalisé en utilisant « un service de communication au public en ligne ». Cela peut renvoyer notamment à la publication de deepfakes sur les réseaux sociaux.

Myriam Quémener, Magistrate et experte auprès du Conseil de l'Europe. Photo : DR

La loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (dite loi SREN) a créé, l'article 226-8-1, qui réprime les délits de montage à caractère sexuel.
Outre l'opportunité d'une adaptation à ce type de publication, la nouvelle loi donne l'occasion de s'interroger sur le positionnement et la pertinence de la protection de la représentation d'une personne dans notre droit actuel.

GI : Existe-t-il des initiatives législatives ou projets en cours visant à renforcer la répression ou la prévention des manipulations par l'intelligence artificielle ?

MQ : Le RIA a été publié au Journal officiel le 12 juillet 2024 et est entré en vigueur le 1er août 2024. Dans ce règlement, l'hypertrucage est définit comme : "une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques".

L'article 50 du RIA pose une obligation de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA. Cet article impose aux personnes générant des deepfakes d'indiquer les contenus qui ont été modifiés ou manipulés grâce à une intelligence artificielle. Lorsque le deepfake fait partie d'une œuvre artistique, créative ou satirique, l'obligation de transparence est atténuée, car cela ne doit pas entraver l'affichage ou la jouissance de l'œuvre.

GI : Au regard des défis technologiques rapides — IA générative, deepfakes, diffusion instantanée — quelles évolutions législatives ou jurisprudentielles vous paraissent prioritaires pour les prochaines années ?

Oui les évolutions sont très rapides. Je pense qu'il faut surtout monter des procédures.

Les principaux textes

Loi SREN — deepfakes et consentements

AI Act — Art. 50 — obligation de transparence pour contenus générés

DSA — obligation de retrait de contenus manipulés

Règlement eIDAS 2 — identité numérique & usurpation d'identité

CJUE / jurisprudence — preuve numérique & réputation

GI : Comment analysez-vous la vague actuelle de réformes dites « Digital omnibus » (NIS 2, DORA, AI Act, RGPD, etc.) ?

MQ : Malgré l'apparence d'un millefeuille législatif en matière de numérique, le fil rouge de tous ces textes est le renforcement de la cybersécurité et par voie de conséquence également le renforcement de la responsabilité des dirigeants.
Il faut relever que la présidence danoise a programmé comme priorité la simplification réglementaire avec la négociation du « Package Omnibus », soutenu par la Commission européenne, visant notamment à modifier le Règlement général sur la protection des données (RGPD) afin de clarifier le cadre juridique pour les entreprises et diminuer toutes les charges inutiles.

GI : Selon vous, quelles sont les principales conséquences pratiques de ces réformes pour les entreprises ?

MQ : Les entreprises doivent se tenir au courant de ces évolutions au besoin en se faisant aider par des juristes. Elles doivent s'adapter et modifier par exemple leur charte informatique pour intégrer par exemple, le recours à l'IA au sein de leurs structures.

GI : Comment les nouvelles obligations peuvent elles impacter les acteurs du numérique ?

MQ : Ces nouvelles obligations impliquent de cartographier les risques et revoir tous les contrats avec les sous traitants.

En anticipant ces évolutions, les entreprises peuvent non seulement éviter les sanctions, mais aussi renforcer leur compétitivité sur un marché mondial de plus en plus exigeant.

GI : Quelles priorités, selon vous, permettraient de renforcer la souveraineté numérique

MQ : Il faut encourager les start up françaises à développer leurs innovations de cybersécurité au niveau national et européen. L'appel à projets France 2030 « Renforcement de l'offre de services Cloud », a pour objectif de soutenir l'émergence de solutions européennes compétitives.
Le lancement d'une mission de préfiguration d'un Observatoire de la souveraineté numérique, confiée au Conseil général de l'Économie a pour but cartographier les dépendances technologiques de la France.
La mobilisation du comité stratégique de filière s'inscrit dans la stratégie européenne d'autonomie stratégique ouverte, fondée sur la coopération, l'innovation et la compétitivité.

INTERVIEW

Ce qui fait dérailler une crise cyber ce n'est pas la technique, mais la gouvernance du discours.

Teddy Ramanakasina, est associé d'un cabinet de taille mondial. Depuis plus de 25 ans, il accompagne les grands groupes internationaux dans la cybersécurité et la conformité pour transformer cette dernière en résilience stratégique.
Il décrypte les angles morts de la communication de crise, la montée en responsabilité des dirigeants et l'impact concret de l'IA sur la vitesse et la complexité des crises.

GI : Quel enseignement majeur tirez-vous de vos interventions auprès de grands groupes confrontés à des crises cyber complexes ? Qu'est-ce qui a le plus changé ces trois dernières années dans la façon de communiquer pendant une cyberattaque ?

TR : Depuis vingt-cinq ans, j'ai vu la crise cyber passer d'un incident "*IT*" à une crise de confiance systémique. Chez Orange, j'ai contribué à sécuriser plus de 40 millions de clients en banque mobile sur 30+ pays. Chez EY, je pilote chaque année plusieurs centaines de revues de risques et de conformité pour des banques et des groupes cotés, souvent dans des contextes de forte pression réglementaire et médiatique.
L'enseignement majeur est simple. Ce qui fait dérailler une crise cyber n'est pas la technique, mais la gouvernance du discours.
Je constate trois évolutions marquantes ces dernières années. Tout d'abord, le temps de réaction s'est effondré. Entre les réseaux sociaux, les fuites sur des forums de cybercriminels et les régulateurs très réactifs, on ne parle plus de "*72h RGPD*", mais souvent de quelques heures pour éviter un vide narratif. Pendant ce temps, le coût moyen mondial d'une violation de données continue de se situer autour de 4,4 à 4,9 M$ par incident, avec des coûts encore plus élevés dans la finance.
Ensuite, la crise n'est plus mono-canal. Un même incident déclenche aujourd'hui :

• un dialogue obligé avec les autorités (CNIL, superviseurs bancaires, etc.) ;
• une attente forte des collaborateurs ;
• des exigences de transparence des clients, médias et parfois ONG.

Teddy Ramanakasina conseille les boards dans les crises - Photo : DR

Un plan de communication qui ne traite que la dimension "*communiqué de presse*" est déjà obsolète.
Ensuite, le board est désormais dans la ligne de mire. Le World Economic Forum rappelle que 91 % des dirigeants considèrent qu'un événement cyber catastrophique est au moins "plausible" à court terme.
Dans le même temps, des études Fortinet et euro-

péennes montrent une hausse des sanctions individuelles contre des dirigeants après attaque (amendes, perte de poste, voire responsabilité personnelle). La communication de crise cyber n'est plus un habillage de la technique, c'est un instrument de gouvernance. Ce qui change, ce n'est pas seulement le ton, c'est le niveau de responsabilité engagé.

GI : Quels sont aujourd'hui les points aveugles les plus fréquents dans les plans de communication de crise ?

TR : Dans les plans que je vois passer chez les grands groupes, y compris très matures, les mêmes angles morts reviennent. Je constate la sous-estimation du facteur temps. Beaucoup de plans restent construits pour une communication séquentielle : "on investigue puis on parle". En pratique, le narratif est souvent déjà en train de se construire ailleurs (forums, presse spécialisée, réseaux sociaux, régulateur). Les organisations continuent de confondre certitude et crédibilité : elles attendent d'être sûres, alors que les parties prenantes attendent qu'elles soient visibles, factuelles et honnêtes sur l'incertitude.

Un autre élément est l'absence de scénario "multi-crise". Les plans sont souvent centrés sur le ransomware "classique". Or les rapports ENISA et Verizon montrent des combinaisons d'extorsion, fuite de données, atteinte à la disponibilité et exploitation de vulnérabilités en chaîne. Les discours ne sont pas préparés pour une crise simultanément réglementaire, financière et réputationnelle.

Le silence mal géré envers les collaborateurs est également à relever. L'interne est trop souvent traité après le régulateur et la presse.

Résultat :

- rumeurs internes,
- captures d'écran qui fuitent,
- perte de confiance dans la direction.

Un plan robuste doit considérer les collaborateurs comme un canal de risque, mais aussi comme un allié de confiance.

J'observe également peu ou pas d'articulation avec les obligations européennes que sont DORA, NIS2, AI Act...

Les textes récents imposent non seulement des délais de notification, mais aussi une cohérence de la narration vis-à-vis des superviseurs. Beaucoup d'organisations ont un plan "*communication corporate*" et un plan "*notification réglementaire*"… qui ne se parlent pas. C'est une source de dissonance, donc de perte de crédibilité.

J'observe également l'absence de répétition réelle au niveau COMEX / CA. Beaucoup de plans sont élégants sur le papier. Mais on constate, comme le WEF, que le nombre d'organisations maintenant une "cyber-résilience minimale" a chuté de 30 %, en particulier pour les petites et moyennes structures. Sans exercices de type "table-top" avec les administrateurs, le plan reste théorique.

GI : Comment cela modifie la vitesse, la nature et la complexité des crises de communication ?

Je vois l'IA agir sur trois axes.

1. Vitesse. Côté attaquants, l'IA générative a industrialisé l'hameçonnage, la rédaction de mails crédibles et la création de contenus trompeurs.
Des analyses récentes montrent que des campagnes de phishing qui demandaient auparavant des heures de préparation peuvent être générées en quelques minutes, avec un taux de personnalisation inédit. Côté défense, les SOC et équipes cyber utilisent l'IA pour corréler les signaux faibles, filtrer les faux positifs et accélérer la détection.
Mais cette accélération des deux côtés crée une asymétrie de compréhension pour les dirigeants : la crise démarre plus vite que leur capacité de cadrage.
2. Nature des crises.
L'IA introduit deux nouvelles dimensions :
• le risque "shadow AI" : outils non référencés utilisés par les métiers, générant des fuites de données et des violations non maîtrisées ;
• le risque lié aux modèles eux-mêmes : biais, erreurs, décisions automatisées difficiles à expliquer.
IBM estime que près d'un cinquième des organisations étudiées ont déjà subi des incidents liés à l'usage non gouverné de l'IA, avec un surcoût significatif sur le coût moyen de la brèche.
En pratique, la communication doit désormais traiter à la fois de la brèche classique et de la question "votre IA a-t-elle contribué au problème ?".
3. Complexité de la narration.
Quand j'interviens sur des sujets IA pour des Boards ou des régulateurs, la difficulté n'est pas d'expliquer l'algorithme ; c'est de traduire en langage de gouvernance :
• Qui est responsable ?
• Les données d'apprentissage étaient-elles maîtrisées ?
• L'IA a-t-elle aggravé la crise ou permis de la détecter ?
Dans un contexte où seulement 14 % des organisations se disent confiantes d'avoir les compétences cyber et IA nécessaires en interne, selon le dernier Outlook du WEF, la tentation est forte de simplifier à l'excès.
Mon point de vue : la bonne réponse n'est pas de simplifier, mais de structurer. C'est là que la gouvernance IA (AI Act, ISO 42001, NIST AI RMF) devient un langage commun utile pour les dirigeants.

GI : Parlons IA. Comment cela modifie la vitesse, la nature et la complexité des crises de communication ?

TR : Je vois l'IA agir sur trois axes. La vitesse. Côté attaquants, l'IA générative a industrialisé l'hameçonnage, la rédaction de mails crédibles et la création de contenus trompeurs. Des analyses récentes montrent que des campagnes de phishing qui demandaient auparavant des heures de préparation peuvent être générées en quelques minutes, avec un taux de personnalisation inédit. Côté défense, les SOC et équipes cyber utilisent l'IA pour corréler les signaux faibles, filtrer les faux positifs et accélérer la détection. Mais cette accélération des deux côtés crée une asymétrie de compréhension pour les dirigeants : la crise démarre plus vite que leur capacité de cadrage.
La nature des crises change. L'IA introduit deux

nouvelles dimensions :

• le risque "shadow AI" : outils non référencés utilisés par les métiers, générant des fuites de données et des violations non maîtrisées ;

• le risque lié aux modèles eux-mêmes : biais, erreurs, décisions automatisées difficiles à expliquer.

IBM estime que près d'un cinquième des organisations étudiées ont déjà subi des incidents liés à l'usage non gouverné de l'IA, avec un surcoût significatif sur le coût moyen de la brèche.

En pratique, la communication doit désormais traiter à la fois de la brèche classique et de la question "votre IA a-t-elle contribué au problème ?".

La complexité de la narration. Quand j'interviens sur des sujets IA pour des Boards ou des régulateurs, la difficulté n'est pas d'expliquer l'algorithme ; c'est de traduire en langage de gouvernance :

• Qui est responsable ?

• Les données d'apprentissage étaient-elles maîtrisées ?

• L'IA a-t-elle aggravé la crise ou permis de la détecter ?

Dans un contexte où seulement 14 % des organisations se disent confiantes d'avoir les compétences cyber et IA nécessaires en interne, selon le dernier Outlook du WEF, la tentation est forte de simplifier à l'excès.

De mon point de vue, la bonne réponse n'est pas de simplifier, mais de structurer. C'est là que la gouvernance IA avec AI Act, ISO 42001, NIST AI RMF… devient un langage commun utile pour les dirigeants.

GI : Deepfakes et identités synthétiques : comment un COMEX peut-il réellement se préparer ?

TR : Les deepfakes ne sont plus un sujet théorique.

En 2024, une équipe de fraudeurs a utilisé une visioconférence deepfake pour imiter un CFO et plusieurs collaborateurs d'un groupe d'ingénierie britannique, entraînant un transfert frauduleux de près de 25–26 M$. Des analyses de marché font état de plus de 100 000 attaques deepfakes signalées sur une seule année aux États-Unis, avec des pertes dépassant 200 M$ sur un trimestre, et des cas récurrents d'imitation de CEO.

Pour un COMEX, la préparation doit être très concrète :

1. Réviser les règles de confiance.

• Toute instruction sensible (transfert, décision stratégique, communication publique) ne doit jamais reposer sur un seul canal numérique temps réel.

• Mettre en place des procédures de "rappel à froid" ou de double validation par un canal indépendant (téléphone connu, confirmation écrite via circuit sécurisé…).

2. Formaliser un protocole "incident deepfake".

• Qui alerte qui lorsqu'un contenu douteux circule ?

• Qui a l'autorité pour confirmer publiquement l'authenticité ou la fausseté d'une vidéo ou d'un audio ?

• Quels canaux sont utilisés pour "réancrer" la réalité (site corporate, comptes officiels, messages vidéo authentifiés) ?

3. Intégrer les deepfakes dans les exercices de crise.

Les simulations que j'anime les plus utiles sont celles où l'on injecte un faux contenu en plein exercice :

• faux message du CEO,
• faux communiqué du régulateur,
• fausse "leak" d'un échange interne.

On voit immédiatement si le COMEX sait garder la tête froide, vérifier, et reprendre la main sur la narration.

4. S'équiper, mais sans naïveté.

Des solutions de détection existent, et certaines commencent à être intégrées dans les SOC, mais les rapports récents montrent qu'aucun outil n'est infaillible.

Le cœur de la défense reste humain et procédural :

• hygiène de vérification systématique,
• culture de doute sain,
• capacité à communiquer vite pour démentir.

GI : Faut-il un "cyber briefing obligatoire" annuel pour les administrateurs, au même titre que les obligations financières ?

TR : Ma réponse est claire : oui, et nous sommes en retard. Plusieurs signaux convergent :

• Une étude de Board Intelligence et du Corporate Governance Institute indique que près de deux tiers des administrateurs n'ont pas reçu de formation suffisante en cyber-résilience dans les 12 derniers mois.

• Les travaux de Fortinet sur le skills gap montrent que près de 87–90 % des organisations ont subi au moins une brèche qu'elles attribuent en partie au manque de compétences cyber, et que plus de la moitié rapportent des sanctions directes contre des dirigeants après attaque. Dans ce contexte, continuer à considérer le cyber comme un "sujet technique" présenté de temps en temps au comité d'audit n'est plus défendable.

Pour moi, un briefing annuel obligatoire devrait respecter trois principes :

1. Être piloté par la gouvernance, pas par la technique.

L'objectif n'est pas d'expliquer le fonctionnement d'un SOC, mais de permettre au CA de :

• comprendre son niveau réel de dépendance numérique,
• se situer par rapport à des benchmarks (coût moyen d'une brèche, fréquence des attaques sectorielles),
• identifier les décisions structurantes à prendre (appétence au risque, budgets, priorités de résilience).

2. Intégrer les régulations structurantes. DORA, NIS2, AI Act, SEC, etc. qui définissent désormais explicitement des responsabilités au niveau du board. Un administrateur doit savoir ce que ces textes impliquent pour lui personnellement et pour le Conseil.

3. Être scénarisé, pas seulement informatif.

Les sessions les plus efficaces que j'ai conduites sont construites autour de scénarios :

• *"votre groupe fait la une pour une fuite massive + un deepfake du CEO"*,
• *"un registre DORA/NIS2 révèle des non-conformités structurelles après incident"*.

L'administrateur se projette, pose les bonnes questions, et comprend où se situent les vrais angles morts. Ce type de briefing n'est pas un luxe : c'est une mesure de protection pour l'entreprise et pour les administrateurs eux-mêmes.

GI : Quel est votre message aux dirigeants et administrateurs qui sous-estiment encore l'ampleur des cyberrisques ?

TR : Je leur dirais trois choses, sans contour. Le risque n'est plus technique. C'est un risque de continuité, de gouvernance et de responsabilité personnelle.

Le WEF, Fortinet et ENISA convergent : les attaques augmentent, la résilience baisse, et les dirigeants sont de plus en plus exposés individuellement après incident. Une cyberattaque n'est plus un "problème DSI" : c'est un événement qui engage le mandat du Conseil, la réputation, et parfois la responsabilité propre des administrateurs.

Ensuite, l'illusion de sécurité par la conformité crée de faux repères. Des audits, des labels, des certifications… et pourtant les brèches continuent. La conformité rassure, mais ne protège pas les décisions stratégiques.

Les plans de communication sont rarement alignés sur les obligations DORA/NIS2, les scénarios IA ne sont pas anticipés, et les deepfakes ne figurent pas encore dans les exercices de crise. Les dirigeants sous-estiment l'effet domino entre communication, régulation, confiance et gouvernance.

Enfin, le Board doit désormais s'appuyer sur un profil hybride, capable de naviguer entre audit, régulation, IA et cyber. C'est le vrai gap du marché.

La plupart des organisations ont :

- des auditeurs qui pensent contrôle,
- des RSSI qui pensent technique,
- des juristes qui pensent conformité,
- des communicants qui pensent narratif.

Mais très peu ont un profil capable d'articuler l'ensemble, de lire les angles morts, et de ramener de la clarté dans un écosystème où les signaux faibles viennent de partout. Un profil hybride — avec une expérience en audit, cybersécurité, IA, réglementation et gestion de crise — est un vecteur de gouvernance. Pas un "expert", mais un capteur de risques systémiques pour le Conseil.

Dans mon expérience auprès de groupes internationaux, c'est ce type de compétence transversale qui permet au Board :

- de comprendre la dynamique réelle d'une crise cyber,
- de structurer les décisions sous incertitude,
- de garder la maîtrise du narratif face aux régulateurs, aux marchés et aux médias,
- d'éviter les décisions émotionnelles qui aggravent la crise.

Mon message, en clair : identifiez ce profil, embauchez-le, structurez-le, et faites-le entrer dans les circuits de décision.

Pas comme une couche technique supplémentaire.

Mais comme une fonction de clarté, au même titre que le contrôle interne ou la conformité financière.

Un Board moderne a besoin de quelqu'un qui :

- comprend l'IA, mais parle gouvernance ;
- comprend la cybersécurité, mais parle risque stratégique ;
- comprend les audits, mais parle décision ;
- comprend la communication de crise, mais parle confiance.

Ce n'est pas un luxe. C'est la condition pour que l'entreprise traverse une crise sans perdre son cap, sa valeur et sa crédibilité.

GOOD INFO CYBER

Votre partenaire stratégique en communication de crise cyber

GOOD INFO cyber

Êtes-vous prêts à communiquer lors d'une crise cyber ?

Nos services

- Diagnostics & Évaluations
- Formations & Serious Games
- Media Training

> Pourquoi Good Info Cyber ?

- Expertise unique, vision intégrée, gain de temps

patrice.cyber@goodinfo.eu - www.goodinfo.eu - Tél. : 06 30 37 14 76

Retrouvez une **boîte à outils complète et gratuite** pour :

+ Évaluer votre préparation à la communication de crise cyber.

+ Réaliser un diagnostic NIS2 pour mesurer votre conformité à la directive.

+ Evaluer votre conformité à l'IA Act

www.goodinfo.eu

GOOD INFO cyber

A propos

Patrice Remeur est fondateur de *Good Info Cyber*, consultant et formateur spécialisé dans la communication de crise cyber. Il accompagne dirigeants, COMEX, collectivités et institutions dans la préparation, la gestion et la mise en place de stratégies face aux crises numériques.

Ambassadeur **MIT Innovators Under 35**, intervenant auprès d'universités et écoles (IMT Atlantique, CESI, INSEEC, ENIB...) et conférencier en Europe et au Canada, il a piloté ou accompagné de nombreux exercices et situations de crise cyber, en lien avec la souveraineté numérique, la conformité (NIS2, DORA, AI Act...) et la gestion de réputation.

Il est également ancien auditeur de l'IHEDN, journaliste et auteur de plusieurs études sectorielles (notamment pour Les Échos Études et Xerfi). Il est à l'initiative de formations dédiées aux décideurs publics et privés sur les nouveaux risques informationnels et la lutte contre les deepfakes.

Avec *Communication de Crise Cyber*, il propose le premier magazine entièrement dédié à la préparation face aux attaques numériques et ainsi, un nouvel outil stratégique pour dirigeants, juristes, RSSI, communicants et décideurs engagés dans la résilience numérique